
UNIVERSITY OF TORONTO
3 1761 01236441 0



LEÇONS SUR CERTAINES QUESTIONS

DE

GÉOMÉTRIE ÉLÉMENTAIRE

F. KLEIN
PROFESSEUR A L'UNIVERSITÉ DE GŒTTINGUE

LEÇONS SUR CERTAINES QUESTIONS

DE

GÉOMÉTRIE ÉLÉMENTAIRE

POSSIBILITÉ DES CONSTRUCTIONS GÉOMÉTRIQUES;
LES POLYGONES RÉGULIERS;
TRANSCENDANCE DES NOMBRES e ET π.
(Démonstration élémentaire)

RÉDACTION FRANÇAISE
autorisée par l'Auteur

PAR

J. GRIESS
ANCIEN ÉLÈVE DE L'ÉCOLE NORMALE SUPÉRIEURE,
PROFESSEUR DE MATHÉMATIQUES AU LYCÉE D'ALGER

PARIS
LIBRAIRIE NONY & Cie
17, RUE DES ÉCOLES, 17

1896

PRÉFACE DU TRADUCTEUR

L'opuscule dont M. Félix Klein a bien voulu m'autoriser à donner une traduction française, est destiné à combler dans une certaine mesure le fossé qui sépare en Allemagne l'enseignement secondaire et l'enseignement supérieur. La transition entre les deux ordres d'enseignement, au point de vue mathématique du moins, se fait plus facilement en France, grâce à l'organisation de nos classes d'Élémentaires supérieures et de Mathématiques spéciales. La plupart des matières qui font partie du programme de cette dernière classe ne s'enseignent en Allemagne que dans les Universités.

Les sujets traités dans les pages suivantes ne figurent pas explicitement dans les programmes de nos grandes écoles; pourtant ils s'y rattachent étroitement. Dans quels cas une construction géométrique est-elle possible ou impossible? Par quels moyens l'est-elle? Qu'est-ce qu'un nombre transcendant? Y a-t-il de tels nombres? Pourquoi les nombres e et π appartiennent-ils à cette catégorie? Autant de questions qu'on ne fait qu'effleurer, ou qu'on ne pouvait aborder, parce que leur solution exigeait la connaissance du calcul intégral.

J'ai pensé qu'il ne serait pas sans intérêt, pour les professeurs et les élèves, de faire connaître de quelle façon claire et précise M. Klein répond à toutes ces questions, par

les moyens les plus simples. La démonstration élémentaire de la transcendance de e est due à M. Gordan, qui l'a publiée, sous une forme très concise, dans les *Mathematische Annalen* ; M. Klein a élucidé d'une façon magistrale tous les détails de la démonstration.

En certains endroits, avec l'autorisation de l'auteur, j'ai librement remanié le texte allemand ; à certaines démonstrations, qui empruntaient le secours de la géométrie analytique, j'ai substitué des démonstrations purement géométriques : la forme du Chapitre IV (Ire partie) a subi ainsi quelques légers changements.

Il va sans dire que j'ai scrupuleusement respecté l'ordre des idées et la marche des démonstrations : les imperfections de forme devront donc être imputées au traducteur seul.

J. GRIESS.

Alger, Septembre 1895.

PRÉFACE

La précision plus grande des définitions, les méthodes de démonstration plus rigoureuses dues à la science moderne sont considérées par la plupart des professeurs de gymnase comme difficiles à comprendre et d'une abstraction exagérée ; par suite elles semblent ne devoir posséder d'importance que pour le cercle restreint des spécialistes.

Je pense différemment. L'été dernier, en une série de leçons de deux heures, devant un auditoire plus considérable que de coutume, j'ai eu le plaisir d'exposer ce que la science moderne nous permet d'affirmer sur la possibilité des constructions de la Géométrie élémentaire. Déjà quelque temps auparavant j'avais eu l'occasion de présenter une esquisse de ces leçons aux auditeurs du cours de vacances qui avait lieu à Gœttingue pendant les vacances de Pâques ; ils y semblèrent prendre un intérêt particulier, et cette impression n'a fait que se confirmer pendant le semestre d'été.

C'est pourquoi je me permets de présenter une courte rédaction de mes leçons comme *écrit de fête* (Festschrift), à l'assemblée de l'*Association pour les progrès de l'enseignement des sciences mathématiques et naturelles*, qui doit se tenir prochainement à Gœttingue. Cette rédaction est due

à M. Taegert, professeur (Oberlehrer) à Ems : il avait pris part au cours de vacances dont j'ai parlé; de plus j'ai pu mettre à sa disposition un cahier de notes prises par plusieurs de mes auditeurs pendant le semestre d'été et revues par moi-même.

Puisse ce petit écrit sans prétention aucune faire du bien dans le sens des efforts de l'association.

Gœttingue, Pâques 1895.

F. KLEIN.

INTRODUCTION

Le présent opuscule doit son existence au désir de rattacher les études mathématiques de l'université à celles des écoles secondaires, et d'établir entre elles un contact plus intime que de coutume. Les leçons qu'on va lire ne sont pourtant pas destinées aux commençants, car les matières qui en font l'objet sont traitées à un point de vue plus élevé que celui où on se place dans l'enseignement élémentaire. Par contre, elles ne supposent que peu de connaissances préliminaires. Il ne sera fait usage que des éléments de l'analyse, par exemple du développement en série de la fonction exponentielle.

Nous allons traiter des constructions géométriques : notre objet ne sera pas la recherche de la solution qui convient à chaque cas particulier, mais plutôt le problème de la possibilité ou de l'impossibilité d'une solution géométrique. Trois problèmes, qui ont déjà fait l'objet des recherches des géomètres anciens, nous intéresseront d'une façon particulière. Ce sont :

1° Le problème de la duplication du cube, appelé aussi le problème de Délos ;

2° La trisection ou division en trois parties égales d'un angle quelconque ;

3° La quadrature du cercle, c'est-à-dire la construction de π.

Les géomètres anciens ont vainement essayé de résoudre

ces problèmes avec la règle et le compas, et c'est précisément parce que leur solution semblait exiger l'intervention de moyens d'un ordre plus élevé, que ces questions sont devenues célèbres. Nous montrerons en effet qu'il est impossible d'en trouver une solution avec la règle et le compas.

L'impossibilité du troisième problème n'a été démontrée qu'à une époque relativement récente. Celle du premier et du second résulte implicitement de la théorie générale de Galois, telle qu'on la trouve développée aujourd'hui dans les traités d'algèbre supérieure. Mais il n'en existe pas de démonstration explicite, sous forme élémentaire, si je fais abstraction des livres d'enseignement de Petersen, qui me semblent d'ailleurs remarquables sous bien d'autres points de vue.

Insistons d'abord sur la différence entre constructions *pratiques* et constructions *théoriques*. S'agit-il de construire un cercle divisé pour un instrument de mesure, cette opération ne se fait en réalité que par tâtonnements. La division exacte du cercle en parties égales (par la règle et le compas) n'était autrefois possible que pour les nombres 2^n, 3, 5 et leurs divers multiples. Gauss y a ajouté d'autres cas en montrant la possibilité de la division en p parties, lorsque p est un nombre premier de la forme

$$p = 2^{2^\mu} + 1,$$

et l'impossibilité de la division dans tous les autres cas.

La pratique ne peut tirer aucun profit de ces résultats ; les considérations de Gauss ont une signification purement théorique ; il en est de même des développements qui font l'objet de ces leçons.

Le premier problème que nous nous proposons est le suivant :

Quels problèmes peut-on ou ne peut-on pas construire géométriquement ?

Précisons d'abord le sens du mot « *construire* », et à cet effet indiquons les instruments dont nous nous servirons le cas échéant. Ce sont :

1° La règle et le compas ;

2° Le compas seul ;

3° La règle seule ;

4° D'autres appareils que nous joindrons à la règle et au compas.

Il est singulier que la géométrie élémentaire ne suffise pas pour répondre à la question posée. Le secours de l'algèbre et de l'analyse devient nécessaire, et il faut par suite nous demander comment s'exprime dans leur langue l'emploi de la règle et du compas pour les constructions. Ce nouveau tour qu'il faut donner à nos idées tient à ce que la géométrie élémentaire ne possède pas de méthode générale, pas d'*algorithme*, comme les deux sciences que nous venons de nommer.

Dans l'analyse on trouve d'abord les opérations *rationnelles*, addition, soustraction, multiplication et division. Deux longueurs étant données, on sait immédiatement exécuter sur elles, au moyen de quatrièmes proportionnelles, ces différentes opérations, à condition de joindre aux longueurs données une longueur unité, dans le cas de la multiplication et de la division.

Nous trouvons ensuite les opérations *irrationnelles* ; elles se divisent en *algébriques* et *transcendantes*. Les opérations algébriques les plus simples sont l'extraction des racines carrées, des racines d'indices supérieurs à 2, la résolution des équations algébriques non résolubles par radicaux, comme celles du 5ᵉ degré et celles de degré supérieur. Comme on sait construire $\sqrt{ab}$, on saura donc construire, avec la règle et le compas, les résultats de toutes les opérations irrationnelles où il n'entre que des racines carrées.

Donc toute formule rationnelle, ou ne renfermant que des

radicaux carrés, peut être construite avec la règle et le compas.

D'autre part, toute construction géométrique *isolée*, qui revient à l'intersection de deux droites, d'une droite et d'un cercle, de deux cercles équivaut à une opération rationnelle ou à l'extraction d'une racine carrée (*).

La construction (par la règle et le compas) des irrationnelles d'ordre supérieur est donc impossible, à moins qu'on ne puisse les ramener à l'extraction d'une suite de racines carrées. Il va de soi que dans toutes les constructions le nombre des opérations doit être limité.

De ce qui précède résulte donc ce théorème fondamental :

La condition nécessaire et suffisante pour qu'une expression analytique puisse être construite avec la règle et le compas, est qu'elle se déduise des grandeurs connues par des opérations rationnelles ou par des racines carrées en nombre fini.

Par conséquent, pour démontrer qu'une grandeur ne peut être construite avec la règle et le compas, il suffira de faire voir que l'équation qui la fournit n'est pas résoluble par un nombre fini de racines carrées.

A plus forte raison en sera-t-il ainsi lorsque l'équation du problème n'est pas algébrique. Un nombre qui ne vérifie aucune équation algébrique, s'appelle un nombre *transcendant*. Ce cas se présente pour les nombres e et π, ainsi que nous le montrerons.

(*) Car au point de vue analytique, l'intersection de deux droites équivaut à la résolution du système

$$ax + by + c = 0,$$
$$a'x + b'y + c' = 0;$$

celle d'une droite et d'un cercle, à celle du système

$$x^2 + y^2 - r^2 = 0,$$
$$ax + by + c = 0;$$

et de même celle de deux cercles ; ces systèmes fournissent manifestement des valeurs rationnelles ou des radicaux carrés. J. G.

PREMIÈRE PARTIE

LA POSSIBILITÉ DE LA CONSTRUCTION DES EXPRESSIONS ALGÉBRIQUES

CHAPITRE I

Équations algébriques résolubles par radicaux carrés.

Les propositions suivantes, tirées de la théorie des équations algébriques, sont probablement connues du lecteur ; nous allons pourtant les démontrer brièvement, afin de mieux faire percevoir l'ensemble des idées.

Si la grandeur à construire x ne dépend que d'expressions rationnelles et de racines carrées, elle est racine d'une équation irréductible $f(x) = 0$, dont le degré est toujours une puissance de 2.

1. Pour avoir une idée nette de la structure de la grandeur x, supposons qu'elle soit de la forme

$$x = \frac{\sqrt{a+\sqrt{c+ef}} + \sqrt{d+\sqrt{b}}}{\sqrt{a}+\sqrt{b}} + \frac{p+\sqrt{q}}{\sqrt{r}},$$

dans laquelle $a, b, c, d, e, f, p, q, r$ sont des expressions rationnelles.

2. Le nombre des radicaux superposés figurant dans un terme de x s'appelle l'*ordre* de ce terme ; l'expression précédente renferme des termes d'ordres 0, 1, 2.

3. μ étant l'ordre maximum, aucun terme ne peut présenter plus de μ radicaux superposés.

4. L'expression

$$x = \sqrt{2} + \sqrt{3} + \sqrt{6}$$

semble renfermer trois termes différents du premier ordre ; mais comme

$$\sqrt{6} = \sqrt{2} \cdot \sqrt{3},$$

elle ne dépend en réalité que de deux termes distincts.

Nous supposerons que cette réduction a été faite dans tous les termes de x, de telle sorte que, parmi les différents termes d'ordre μ, aucun ne peut s'exprimer rationnellement en fonction des autres termes d'ordre μ ou d'ordre inférieur.

Nous ferons la même hypothèse sur les termes d'ordre $\mu - 1$ ou d'ordre inférieur ; ces termes peuvent d'ailleurs se présenter explicitement ou implicitement. Cette hypothèse, évidemment très naturelle, est d'une grande importance pour les conclusions ultérieures.

5. *Forme normale de x.*

Si l'expression x est une somme de termes de dénominateurs différents, on les réduira au même dénominateur ; x se présente alors sous la forme du quotient de deux fonctions entières.

Soit $\sqrt{Q}$ un des termes d'ordre μ ; il ne peut figurer dans x que sous forme explicite, puisque μ est l'ordre maximum. D'autre part les puissances de Q s'expriment en fonction de $\sqrt{Q}$ et de Q qui est un terme d'ordre inférieur à μ. La valeur de x peut donc se ramener à la forme

$$x = \frac{a + b\sqrt{Q}}{c + d\sqrt{Q}} ;$$

a, b, c, d ne contiennent plus que $(n - 1)$ termes d'ordre μ et les termes d'ordre inférieur.

Multipliant les deux termes par $c - d\sqrt{Q}$, le dénomi-

nateur ne contient plus $\sqrt{Q}$; il vient

$$x = \frac{ac - bdQ + (bc - ad)\sqrt{Q}}{c^2 - d^2Q} = \alpha + \beta\sqrt{Q} ;$$

α et β ne renferment plus que $n - 1$ termes d'ordre μ.

Si on avait considéré un autre terme d'ordre μ, par exemple $\sqrt{Q_1}$, on aurait de même pu ramener la valeur de x à la forme

$$x = \alpha_1 + \beta_1\sqrt{Q_1}, \quad \text{etc.}$$

On peut donc transformer x de manière que cette expression ne renferme un terme donné d'ordre μ qu'à son numérateur et qu'elle ne le contienne que linéairement.

Remarquons d'ailleurs que, dans cette transformation, peuvent figurer les produits des termes d'ordre μ. En effet, α et β dépendent encore de $n - 1$ termes d'ordre μ. On pourra donc faire en sorte que

$$\alpha = \alpha_{11} + \alpha_{12}\sqrt{Q_1}, \qquad \beta = \beta_{11} + \beta_{12}\sqrt{Q_1},$$

et par suite

$$x = (\alpha_{11} + \alpha_{12}\sqrt{Q_1}) + (\beta_{11} + \beta_{12}\sqrt{Q_1})\sqrt{Q}.$$

6. Nous procéderons d'une façon analogue pour les différents termes d'ordre $\mu - 1$, qui se présentent explicitement dans Q, Q_1, etc.; chacune de ces quantités devient alors une fonction linéaire et entière par rapport au terme d'ordre $\mu - 1$ considéré. Nous passons ensuite aux termes d'ordre inférieur, et nous finissons ainsi par mettre x et ses termes des divers ordres sous forme de fonctions rationnelles, linéaires et entières, par rapport aux radicaux qui y figurent *explicitement*. Nous dirons alors que x est mis sous la *forme normale*.

7. Soit m le nombre total des radicaux carrés indépendants (4) qui figurent dans cette forme normale. En attribuant le double signe à ces radicaux et les combinant de toutes les manières possibles, nous obtiendrons un système

de 2^m valeurs,

$$x_1, x_2, \ldots, x_{2^m},$$

qui seront désignées par le nom de *valeurs conjuguées*. Nous allons chercher une équation admettant ces valeurs conjuguées comme racines.

8. Ces valeurs ne sont pas nécessairement toutes distinctes; car, si on a par exemple

$$x = \sqrt{a + \sqrt{b}} + \sqrt{a - \sqrt{b}},$$

cette expression ne change pas quand on change le signe de $\sqrt{b}$.

9. Formons le polynome

$$F(x) = (x - x_1)(x - x_2) \ldots (x - x_{2^m}).$$

L'équation $F(x) = 0$ admet évidemment pour racines les différentes valeurs conjuguées; elle est du degré 2^m, mais peut admettre des racines multiples (8).

Les coefficients du polynome $F(x)$, *ordonné par rapport à* x, *sont rationnels.*

Changeons en effet le signe d'un des radicaux carrés, ce qui a pour effet de permuter deux racines, x_λ et $x_{\lambda'}$ par exemple, puisque les racines de $F(x)$ sont précisément toutes les valeurs conjuguées. Comme ces racines n'entrent dans $F(x)$ que sous la forme du produit

$$(x - x_\lambda)(x - x_{\lambda'}),$$

on ne fait que changer l'ordre des facteurs de $F(x)$; donc ce polynome ne change pas.

$F(x)$ reste donc invariable quand on change le signe de l'une quelconque des racines carrées; il ne contient donc que leurs carrés; il en résulte bien que ses coefficients sont rationnels.

10. *Lorsque l'une quelconque des valeurs conjuguées vérifie une équation à coefficients rationnels* $f(x) = 0$, *il en est de même de toutes les autres.*

$f(x)$ n'est pas nécessairement égal à $F(x)$, et peut admettre d'autres racines en dehors des x_i.

Soit $x_1 = \alpha + \beta\sqrt{Q}$ une des grandeurs conjuguées, $\sqrt{Q}$ un terme d'ordre μ; α et β dépendent encore des autres termes d'ordre μ et des termes d'ordre inférieur. Il existe alors une grandeur conjuguée

$$x'_1 = \alpha - \beta\sqrt{Q}.$$

Exprimons que x_1 satisfait à l'équation $f(x) = 0$. Mettons $f(x_1)$ par rapport à $\sqrt{Q}$ sous la forme normale

$$f(x_1) = A + B\sqrt{Q};$$

cette expression ne peut être nulle que sous les conditions simultanées

$$A = 0, \qquad B = 0;$$

s'il en était autrement, on aurait

$$\sqrt{Q} = -\frac{A}{B};$$

on pourrait donc exprimer $\sqrt{Q}$ rationnellement en fonction des termes d'ordre μ et des termes d'ordre inférieur contenus dans A et B, ce qui est contraire à l'hypothèse de l'indépendance de toutes les racines carrées (4).

Mais on a évidemment

$$f(x'_1) = A - B\sqrt{Q};$$

si donc $f(x_1)$ est nul, il en est de même de $f(x'_1)$. D'où cette première proposition :

Si la grandeur x_1 satisfait à l'équation $f(x) = 0$, il en est de même de toutes les valeurs conjuguées qui se déduisent de x_1 par le changement de signe de l'un des termes d'ordre μ.

La démonstration se fait d'une manière analogue pour les autres valeurs conjuguées. Supposons par exemple (ce qui ne restreint pas la généralité du raisonnement) que l'expression x ne dépende que de deux termes d'ordre μ, $\sqrt{Q}$ et $\sqrt{Q'}$. $f(x_1)$ pourra être ramenée à la forme normale suivante :

$$(a) \qquad f(x_1) = p + q\sqrt{Q} + r\sqrt{Q'} + s\sqrt{Q}\,.\sqrt{Q'} = 0.$$

Si x dépendait de plus de deux termes d'ordre μ, il faudrait adjoindre à l'expression précédente un plus grand nombre de termes de structure analogue.

L'équation (a) n'est possible que si l'on a séparément

$$(b) \qquad p = 0, \quad q = 0, \quad r = 0, \quad s = 0,$$

sans quoi $\sqrt{Q}$ et $\sqrt{Q'}$ seraient liés par une relation rationnelle, ce qui est contraire à l'hypothèse (4).

Soient maintenant $\sqrt{R}$ et $\sqrt{R'}$ les termes d'ordre $\mu - 1$ dont dépend x_1; ils figurent dans p, q, r, s; on pourra donc mettre ces quantités sous la forme normale par rapport à $\sqrt{R}$ et $\sqrt{R'}$ (en supposant qu'il n'y en ait que deux). On obtient ainsi des équations de la forme

$$(c) \qquad p = k_1 + l_1\sqrt{R} + m_1\sqrt{R'} + n_1\sqrt{RR'} = 0$$

et d'autres équations analogues pour q, r, s.

L'hypothèse, déjà plusieurs fois utilisée, de l'indépendance des radicaux, nous donne de suite les conditions

$$k_1 = 0, \quad l_1 = 0, \quad m_1 = 0, \quad n_1 = 0, \quad \text{etc.}$$

Il en résulte que les équations (c) et par suite aussi $f(x) = 0$, sont vérifiées, lorsque, au lieu de x_1, on emploie les valeurs conjuguées qui s'en déduisent par les changements de signe de $\sqrt{R}$ et $\sqrt{R'}$. Donc :

L'équation $f(x) = 0$ est aussi vérifiée par toutes les valeurs conjuguées qui se déduisent de x_1 en changeant le signe de l'un des termes d'ordre $\mu - 1$.

Le même procédé de démonstration s'applique évidemment aux termes d'ordre $\mu - 2$, $\mu - 3$, etc., ce qui prouve entièrement la proposition énoncée.

11. Nous venons de considérer deux équations

$$F(x) = 0 \qquad \text{et} \qquad f(x) = 0,$$

à coefficients rationnels, admettant toutes deux comme racines les quantités x_i.

$F(x)$ est du degré 2^m, et peut avoir des racines multiples ; $f(x)$ peut avoir d'autres racines que les x_i.

Soit $\varphi(x) = 0$ l'équation de moindre degré, à coefficients rationnels, admettant la racine x_1 et par suite toutes les quantités x_i (10).

12. *Propriétés de l'équation* $\varphi(x) = 0$.

I. $\varphi(x) = 0$ *est une équation irréductible.*

Cela veut dire que son premier membre ne peut être mis sous forme d'un produit de deux polynomes à coefficients rationnels.

Si on avait en effet

$$\varphi(x) = \psi(x)\chi(x),$$

la condition $\varphi(x_1) = 0$ entraînerait

$$\psi(x_1) = 0 \qquad \text{ou} \qquad \chi(x_1) = 0.$$

Mais, d'après (10), si x_1 satisfait à l'équation à coefficients rationnels $\psi(x) = 0$, il en est de même de toutes les valeurs conjuguées x_i ; $\varphi(x) = 0$ ne serait donc pas l'équation *du moindre degré* ayant les x_i pour racines.

II. $\varphi(x) = 0$ *n'a pas de racines multiples.*

Car si elle en avait, son premier membre $\varphi(x)$ pourrait se décomposer en facteurs rationnels d'après les méthodes connues de l'Algèbre (*) ; donc $\varphi(x) = 0$ ne serait pas irréductible.

III. $\varphi(x) = 0$ *n'admet pas d'autres racines que les quantités* x_i.

S'il en était autrement, $F(x)$ et $\varphi(x)$ admettraient un plus grand commun diviseur, qu'on sait calculer rationnellement. On pourrait donc décomposer $\varphi(x)$ en facteurs rationnels, ce qui est impossible, puisque $\varphi(x)$ est irréductible.

(*) Théorie des Racines égales.

IV. Soit M le nombre des x_i qui ont des valeurs distinctes, et soient

$$x_1, x_2, \ldots, x_m$$

ces quantités ; on aura

$$\varphi(x) = C(x - x_1)(x - x_2) \ldots (x - x_m).$$

En effet, l'équation $\varphi(x) = 0$ admet pour racines les quantités $x_1, \ldots, x_m$; elle n'admet pas de racines multiples ; le polynome $\varphi(x)$ est donc déterminé à un facteur constant près, dont la valeur n'importe pas pour l'équation

$$\varphi(x) = 0.$$

V. *$\varphi(x) = 0$ est la seule équation irréductible à coefficients rationnels admettant les x_i pour racines.*

Car si $f(x) = 0$ était une autre équation rationnelle irréductible admettant comme racine x_1 et par suite toutes les quantités x_i, $f(x)$ devrait être divisible par $\varphi(x)$ et par suite ne serait pas irréductible.

13. Comparons maintenant $F(x)$ et $\varphi(x)$. — Ces deux polynomes ont pour seules racines les x_i, et en outre $\varphi(x)$ n'admet pas de racines multiples. $F(x)$ est donc divisible par $\varphi(x)$:

$$F(x) = F_1(x).\varphi(x).$$

$F_1(x)$ a nécessairement ses coefficients rationnels, comme étant le quotient de la division de $F(x)$ par $\varphi(x)$. Si ce n'est pas une constante, ce polynome admet des racines appartenant à $F(x)$; en admettant au moins une, il les admettra toutes (10). Donc $F_1(x)$ est aussi divisible par $\varphi(x)$, et

$$F_1(x) = F_2(x).\varphi(x).$$

Si $F_2(x)$ n'est pas une constante, le même raisonnement est encore applicable. Le degré des polynomes quotient s'abaisse à chaque opération ; par suite au bout d'un nombre limité de divisions on tombe sur une égalité de la forme

$$F_{n-1}(x) = C.\varphi(x).$$

Multipliant toutes les égalités obtenues membre à membre, il vient

$$F(x) = C.[\varphi(x)]^n.$$

Donc :

Le polynome $F(x)$ est une puissance du polynome de degré minimum $\varphi(x)$, abstraction faite d'une certaine constante.

14. Nous pouvons maintenant nous rendre compte du degré de $\varphi(x)$. $F(x)$ est du degré 2^m ; c'est de plus la n^e puissance de $\varphi(x)$, lequel est du degré M ; il en résulte que

$$2^m = n.M.$$

Donc M est une puissance de 2 ; remarquons qu'il en est de même de n. D'où ce théorème :

Le degré de l'équation irréductible à coefficients rationnels, à laquelle satisfait une expression ne dépendant que de radicaux carrés, est une puissance de 2.

15. Comme, d'autre part, il n'existe qu'une seule équation irréductible à coefficients rationnels, vérifiée par tous les x_i, il en résulte la réciproque suivante :

Si une équation irréductible n'est pas du degré 2^h, elle ne peut certainement pas être résolue par radicaux carrés.

CHAPITRE II

Le problème de Délos et la trisection d'un angle quelconque.

1. Appliquons les théorèmes du chapitre précédent au problème de Délos ou de la duplication du cube. Étant donné un cube dont l'arête est prise pour unité de longueur, il s'agit de trouver l'arête x d'un second cube dont le volume soit double de celui du premier. L'équation du problème est évidemment

$$x^3 - 2 = 0.$$

Cette équation est irréductible; car si elle ne l'était pas, son premier membre pourrait se décomposer en facteurs rationnels, dont l'un au moins serait du premier degré en x. Il existerait donc une valeur rationnelle pour $\sqrt[3]{2}$, ce qui n'est pas.

D'autre part, le degré de cette équation n'est pas de la forme 2^h; donc ses racines ne peuvent s'exprimer uniquement à l'aide de racines carrées en nombre fini. Par suite il est impossible de les construire, c'est-à-dire de résoudre le problème proposé avec la règle et le compas.

2. Considérons maintenant l'équation plus générale

$$x^3 - \lambda = 0,$$

λ désignant un paramètre, qui peut être une quantité complexe de la forme $a + bi$. Cette équation traduit analytiquement, ainsi que nous le verrons, aussi bien le problème de la multiplication du cube que celui de la trisection d'un angle quelconque.

Il s'agit de reconnaître si cette équation est irréductible,

c'est-à-dire si l'une de ses racines se présente sous la forme d'une fonction rationnelle de λ.

Remarquons en passant que l'irréductibilité d'une expression dépend en général des grandeurs qu'on suppose connues. Dans l'équation $x^3 - 2 = 0$, il s'agit de grandeurs numériques ; on se demande si $\sqrt[3]{2}$ peut avoir une valeur numérique rationnelle. Pour l'équation $x^3 - \lambda = 0$, on se demande si une racine de cette équation peut être représentée par une fonction rationnelle de λ. Dans le premier cas, le *domaine de rationalité* comprend l'ensemble des nombres rationnels ; dans le second cas, il est formé par les fonctions rationnelles d'un paramètre.

Ce paramètre étant supposé indépendant, on voit immédiatement qu'aucune expression de la forme $\frac{\varphi(\lambda)}{\psi(\lambda)}$, dans laquelle $\varphi(\lambda)$ et $\psi(\lambda)$ sont des polynomes, ne peut vérifier notre équation. L'équation considérée est donc irréductible, et, comme son degré n'est pas de la forme 2^h, elle n'est pas résoluble à l'aide de radicaux carrés.

3. Restreignons maintenant la variabilité de λ. Posons (*fig.* 1)

$$\lambda = r(\cos\varphi + i\sin\varphi),$$

d'où

$$\sqrt[3]{\lambda} = \sqrt[3]{r}\sqrt[3]{\cos\varphi + i\sin\varphi}.$$

Notre problème se décompose en deux : extraire la racine cubique d'un nombre réel et celle d'un nombre imaginaire de la forme $\cos\varphi + i\sin\varphi$, ces nombres étant d'ailleurs quelconques. Nous allons traiter séparément ces deux problèmes.

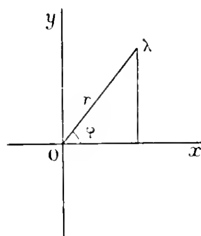


Fig. 1

1. Les racines de l'équation

$$x^3 - r = 0$$

sont

$$\sqrt[3]{r}, \quad \varepsilon\sqrt[3]{r}, \quad \varepsilon^2\sqrt[3]{r},$$

en représentant par ε et ε^2 les racines cubiques imaginaires de l'unité,

$$\varepsilon = \frac{-1 + i\sqrt{3}}{2}, \qquad \varepsilon^2 = \frac{-1 - i\sqrt{3}}{2}.$$

En prenant pour domaine de rationalité l'ensemble des fonctions rationnelles de r, on sait, d'après un raisonnement précédent (2), que l'équation

$$x^3 - r = 0$$

est irréductible. Par suite le problème de la multiplication du cube n'est pas susceptible, en général, d'une solution géométrique avec la règle et le compas.

II. Les racines de l'équation

$$x^3 - (\cos\varphi + i \sin\varphi) = 0$$

sont, d'après la formule de Moivre,

$$x_1 = \cos\frac{\varphi}{3} + i \sin\frac{\varphi}{3},$$

$$x_2 = \cos\frac{2\pi + \varphi}{3} + i \sin\frac{2\pi + \varphi}{3},$$

$$x_3 = \cos\frac{4\pi + \varphi}{3} + i \sin\frac{4\pi + \varphi}{3}.$$

Ces racines se représentent géométriquement (*fig.* 2) par les sommets d'un triangle équilatéral, inscrit dans un cercle de rayon 1, ayant l'origine pour centre. La figure montre qu'à la racine x_1 correspond l'argument $\frac{\varphi}{3}$; l'équation considérée est donc l'expression analytique du problème de la trisection de l'angle.

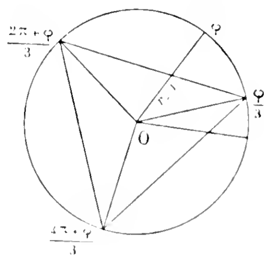


Fig. 2

Si l'équation

$$x^3 - (\cos\varphi + i \sin\varphi) = 0$$

était réductible, l'une au moins de ses racines devrait pouvoir être représentée par une fonction rationnelle de $\cos\varphi$ et $\sin\varphi$. Par suite sa valeur ne changerait pas en remplaçant φ par $2\pi+\varphi$.

Mais, si on opère ce changement par une variation continue de l'angle φ, on voit que les racines x_1, x_2, x_3 se permutent circulairement.

Par conséquent nulle racine ne peut être représentée par une fonction rationnelle de $\cos\varphi$ et de $\sin\varphi$. Donc l'équation proposée est irréductible, et, comme son degré n'est pas de la forme 2^h, elle n'est pas résoluble à l'aide de racines carrées en nombre fini. *La trisection de l'angle ne peut donc se faire avec la règle et le compas.*

Cette démonstration, de même que le théorème général, n'est valable que si φ est un angle arbitraire; pour certaines valeurs particulières de φ la construction peut se trouver possible.

CHAPITRE III

La division du cercle en parties égales.

1. La division du cercle en n parties égales a fait l'objet des recherches des anciens ; on sait depuis longtemps résoudre le problème lorsque n est égal à l'un des nombres 2^h, 3, 5 ou à l'un de leurs multiples communs.

Dans ses *Disquisitiones arithmeticæ*, Gauss a augmenté le nombre des entiers pour lesquels la solution est possible, en montrant que la division peut se faire pour tout nombre premier de la forme

$$(1) \qquad p = 2^{2^\mu} + 1,$$

et qu'elle est impossible pour tous les autres nombres premiers et leurs puissances.

Si, dans l'équation (1), on donne à μ les valeurs 0 et 1, on trouve pour p les valeurs 3 et 5, cas qui étaient déjà connus des géomètres anciens. Pour $\mu = 2$, on trouve

$$p = 2^{2^2} + 1 = 17 ;$$

ce cas a été complètement traité par Gauss.

Pour $\mu = 3$, on trouve

$$p = 2^8 + 1 = 257,$$

qui est un nombre premier; on sait donc construire le polygone régulier de 257 côtés.

Il en est de même pour $\mu = 4$, car

$$2^{2^4} + 1 = 65537$$

est un nombre premier.

Les valeurs 5, 6, 7 attribuées à μ ne donnent pas de nombres premiers. Personne n'a encore examiné le cas de $\mu = 8$; il ne faut pas s'en étonner. Il a fallu en effet de

patients efforts et une ingéniosité singulière pour démontrer que les grands nombres correspondant à $\mu = 5, 6, 7$ ne sont pas premiers. Il est donc possible que $\mu = 4$ soit le dernier nombre pour lequel une solution soit possible.

Richelot a publié un travail considérable sur le polygone régulier de 257 côtés, dans le *Journal de Crelle*, t. IX, 1832, p. 1-26, 146-161, 209-230, 337-356. Son mémoire est intitulé :

De resolutione algebraica æquationis

$$x^{257} = 1,$$

sive de divisioni circuli per trisectionem anguli septies repetitam in partes 257 inter se æquales commentatio coronata.

M. Hermes, professeur à Lingen, a consacré dix ans à des recherches sur le polygone régulier de 65537 côtés; il a examiné avec soin toutes les racines qui se présentent d'après la méthode de Gauss. L'ensemble considérable de ces recherches est conservé dans les collections du séminaire mathématique de Gœttingue. On peut se reporter à une communication de M. le Professeur Hermes dans le n° 3 des « *Gœttinger Nachrichten* » (1894).

2. On peut restreindre le problème de la division du cercle en n parties égales au cas où n est un nombre premier p ou une puissance p^α d'un tel nombre. En effet, si n est un nombre composé, et si μ et ν sont des facteurs de n premiers entre eux, on peut toujours trouver des entiers a et b positifs ou négatifs, tels que

$$1 = a\mu + b\nu,$$

d'où,
$$\frac{1}{\mu\nu} = \frac{a}{\nu} + \frac{b}{\mu}.$$

Pour diviser le cercle en $\mu\nu = n$ parties égales, il suffit de savoir le diviser respectivement en μ et ν parties égales. Ainsi pour $n = 15$, on a

$$\frac{1}{15} = \frac{2}{3} - \frac{3}{5}.$$

3. Démontrons d'abord la proposition suivante :

Lorsqu'un nombre premier est de la forme

$$2^h + 1,$$

on a nécessairement $h = 2^\alpha$.

Nous nous appuierons pour cela sur le théorème de Fermat :

Si p *est un nombre premier, et* a *un entier non divisible par* p, *ces nombres vérifient la congruence*

$$a^{p-1} \equiv +1 \qquad (\text{mod. } p)\ (*)$$

$p-1$ n'est pas nécessairement le plus petit exposant qui, pour une valeur donnée de a, vérifie la congruence. Soit s ce moindre exposant ; on démontre que s est un diviseur de $p-1$ (**). Si en particulier s est égal à $p-1$, on dit que a est une *racine primitive* de p ; remarquons en passant que pour chaque nombre premier p il y a nécessairement une racine primitive. Nous ne ferons d'ailleurs usage de cette considération que plus tard.

Soient donc p un nombre premier tel que

(*) $a \equiv b$ (mod. p) s'énonce a congru à b module p et signifie que la différence $a - b$ est divisible par p. La congruence ci-dessus signifie donc que $a^{p-1} - 1$ est divisible par p. C'est l'énoncé du théorème de Fermat tel qu'on le donne dans les traités élémentaires. On peut ajouter, soustraire, multiplier, diviser membre à membre des congruences de même module, élever au carré les deux membres d'une congruence.

On pourra consulter à ce sujet les Leçons d'Arithmétique de M. Tannery, p. 454 et suivantes, de M. Humbert, p. 162 et suivantes.

J. G.

(**) Soient q et r le quotient et le reste de la division de $p-1$ par s, de sorte que

$$p - 1 = sq + r,$$

donc

$$a^{p-1} = a^{sq}.a^{r}.$$

Comme, par hypothèse,

$$a^{s} \equiv +1 \qquad (\text{mod. } p),$$

on a aussi

$$a^{sq} \equiv +1 \qquad (\text{mod. } p),$$

et par suite

$$a^{p-1-sq} \equiv a^{r} \equiv +1 \qquad (\text{mod. } p).$$

Or r est inférieur à s ; et s est par hypothèse le plus petit entier vérifiant la congruence

$$a^{x} \equiv +1 \qquad (\text{mod. } p).$$

Donc $r = 0$, et

$$p - 1 = sq.$$

J. G.

(1) $$p = 2^h + 1,$$

et s le plus petit entier tel que

(2) $$2^s \equiv + 1 \pmod{p}.$$

L'égalité (1) montre que $2^h < p$; la congruence (2) exige que $2^s > p$; donc

$$s > h.$$

L'égalité (1) montre que h est le plus petit entier vérifiant la congruence

(3) $$2^h \equiv - 1 \pmod{p}.$$

De (2) et (3) on tire par division

$$2^{s-h} \equiv - 1 \pmod{p};$$

donc

(4) $$s - h \geqq h, \qquad s \geqq 2h.$$

D'autre part, on conclut de (3) par élévation au carré

$$2^{2h} \equiv 1 \pmod{p}.$$

Comparant à (2), et tenant compte de ce que s est le plus petit exposant vérifiant les congruences de la forme

$$2^r \equiv 1 \pmod{p},$$

il vient

(5) $$s \leqq 2h.$$

Les conditions (4) et (5) devant être remplies simultanément, on a nécessairement

$$s = 2h.$$

Or on a remarqué que s est un diviseur de $p - 1 = 2^h$, il en est donc de même de h, qui, par suite, est une puissance de 2.

Donc les nombres premiers de la forme $2^h + 1$ sont nécessairement de la forme

$$2^{2^\mu} + 1.$$

4. Ce résultat peut encore s'établir de la manière suivante.

Supposons que h soit divisible par un nombre impair, de telle sorte que

$$h = h'(2n + 1).$$

On sait que
$$x^{2n+1}+1=(x+1)(x^{2n}-x^{2n-1}+\cdots+1).$$
Remplaçons x par $2^{h'}$: on voit que le nombre
$$2^{h'(2n+1)}+1=2^h+1$$
serait divisible par $2^{h'}+1$; par conséquent il ne peut représenter un nombre premier.

5. Arrivons maintenant à notre proposition fondamentale :

p étant un nombre premier, la division du cercle en p parties égales, au moyen de la règle et du compas, est impossible si p n'est pas de la forme
$$p=2^h+1=2^{2^\mu}+1.$$

Posons $z=x+iy$; traçons dans le plan de la variable z un cercle de rayon 1. Diviser ce cercle en n parties égales revient à résoudre l'équation binome
$$z^n-1=0.$$
Cette équation admet la racine $z=1$; supprimons-la en divisant par $z-1$, ce qui revient, géométriquement, à ne pas considérer le point de départ de la division. Il reste alors à résoudre l'équation
$$z^{n-1}+z^{n-2}+\ldots+z+1=0,$$
que nous appellerons l'*équation de division*.

Or, quand n est égal à un nombre premier p, cette équation est irréductible (nous allons le démontrer ci-après) ; elle ne peut donc être résolue à l'aide de radicaux carrés en nombre fini que lorsque son degré est une puissance de 2 (Chap. I, 15). Il faut donc que
$$n-1=p-1=2^h,$$
ou bien
$$p=2^h+1,$$
et par suite
$$p=2^{2^\mu}+1.$$
On voit que les nombres premiers, signalés par Gauss, jouent un rôle tout particulier.

6. Reste donc à faire voir que l'équation de division est irréductible.

Lemme de Gauss.

Lorsqu'un polynome rationnel et entier, à coefficients entiers (*), *peut être décomposé en un produit de deux facteurs rationnels, les coefficients de ces facteurs sont aussi des nombres entiers.*

Soit

$$F(z) = z^m + Az^{m-1} + Bz^{m-2} + \cdots + Lz + M$$

ce polynome ; A, B, C, ..., M sont des nombres entiers. Par hypothèse ce polynome peut se mettre sous la forme

$$(1) \quad F(z) = f(z).\varphi(z) = (z^{m'} + \alpha_1 z^{m'-1} + \cdots)(z^{m''} + \beta_1 z^{m''-1} + \cdots).$$

Il s'agit de faire voir que les coefficients α_i et β_i sont des nombres entiers.

Supposons qu'ils soient fractionnaires. Réduisons dans chaque facteur tous les coefficients au même dénominateur ; soient a_0 et b_0 ces dénominateurs communs. Multiplions ensuite les deux membres de notre égalité par $a_0 b_0$; elle prend la forme

$$a_0 b_0 F(z) = f_1(z)\varphi_1(z) = (a_0 z^{m'} + a_1 z^{m'-1} + \cdots)(b_0 z^{m''} + b_1 z^{m''-1} + \cdots).$$

Les coefficients a sont des nombres premiers entre eux et de même les b, puisque par hypothèse a_0 et b_0 sont les plus petits communs dénominateurs.

Supposons a_0 et b_0 différents de l'unité, et soit q un diviseur premier de $a_0 b_0$. Soient de plus a_i le premier coefficient de $f_1(z)$ et b_k le premier coefficient de $\varphi_1(z)$, non divisibles par q. Développons le produit $f_1(z)\varphi_1(z)$ et cherchons le coefficient de $z^{m'+m''-i-k}$. Ce sera

$$a_i b_k + a_{i-1} b_{k+1} + \cdots + a_{i+1} b_{k-1} + a_{i+2} b_{k-2} + \cdots$$

D'après nos hypothèses, tous les termes à partir du second

(*) Ayant l'unité pour coefficient de son terme de plus haut degré.

sont divisibles par q ; le premier ne l'est pas ; donc ce coefficient n'est pas divisible par q. Or le coefficient de $z^{m'+m''-i-k}$ dans le premier membre est divisible par $a_0 b_m$, c'est-à-dire par q. Donc si l'identité est vraie, il est impossible que dans chaque polynome il existe un coefficient non divisible par q.

Les coefficients de l'un au moins des polynomes sont donc tous divisibles par q. C'est là une autre impossibilité, puisque nous avons vu que tous ces coefficients sont premiers entre eux.

Donc on ne peut supposer a_0 et b_0 différents de 1 ; et par suite les coefficients α_i et β_i sont entiers.

7. *L'équation de division est irréductible.*

Comme le coefficient de son premier terme est égal à l'unité, il suffit, d'après le lemme de Gauss, de montrer que son premier membre ne peut se décomposer en deux facteurs dont les coefficients soient entiers. Nous nous servirons à cet effet de la méthode d'Eisenstein (*Journal de Crelle*, 39, p. 67), qui consiste à faire la substitution

$$z = x + 1.$$

Il vient alors

$$f(z) = \frac{z^p - 1}{z - 1} = \frac{(x+1)^p - 1}{x} = x^{p-1} + px^{p-2}$$
$$+ \frac{p(p-1)}{1.2} x^{p-3} + \cdots + \frac{p(p-1)}{1.2} x + p = 0.$$

Tous les coefficients du second membre, sauf le premier, sont divisibles par p ; le dernier coefficient est toujours égal à p qui, par hypothèse, est un nombre premier. Une expression de ce genre est toujours irréductible.

En effet, s'il n'en était pas ainsi, on aurait

$$f(x+1) = (x^{m'} + a_1 x^{m'-1} + \cdots + a_{m'-1} x + a_{m'})$$
$$(x^{m''} + b_1 x^{m''-1} + \cdots + b_{m''-1} x + b_{m''}),$$

les coefficients a et les coefficients b étant des nombres entiers.

Les termes indépendants de x devant être égaux, on a

$$a_m b_{m'} = p;$$

p étant un nombre premier, l'un des facteurs du premier membre doit être égal à 1 ; supposons donc que

$$a_m = \pm p, \qquad b_{m'} = \pm 1.$$

Égalons ensuite les coefficients des termes en x ; il vient

$$\frac{p(p-1)}{1.2} = a_{m-1}b_{m'} + a_m b_{m'-1}.$$

Le premier membre et le second terme du second membre sont divisibles par p ; il doit donc en être de même de $a_{m-1}b_{m'}$; comme $b_{m'} = \pm 1$, a_{m-1} est divisible par p.

Égalant ensuite les coefficients des termes en x^2, il vient

$$\frac{p(p-1)(p-2)}{1.2.3} = a_{m-2}b_{m'} + a_{m-1}b_{m'-1} + a_{m-2}b_{m'-2};$$

on en conclut que a_{m-2} est divisible par p.

On continuerait ainsi de proche en proche ; le coefficient du terme en x^m serait

$$a_0 b_{m'} + a_1 b_{m'-1} + \cdots;$$

avant d'arriver à ce coefficient, on a démontré que a_m, $a_{m-1}, \ldots a_1$ sont divisibles par p ; on en conclut que a_0 doit aussi être divisible par p, ce qui est impossible puisque $a_0 = 1$.

L'égalité supposée est donc impossible, et par suite l'équation de division est irréductible, lorsque p est un nombre premier.

8. *Cas où n est égal à une puissance d'un nombre premier.*

Soit $n = p^2$; nous allons montrer que si p est plus grand que 2, la division du cercle en p^2 parties égales est impossible. Le problème sera résolu par là même pour $\alpha > 2$; car la division en p^α parties égales comprend évidemment la division en p^2 parties égales.

L'équation de division est ici

$$\frac{z^{p^2}-1}{z-1}=0\,;$$

elle admet comme racines étrangères au problème celles qui conviennent à la division en p parties égales, c'est-à-dire les racines de l'équation

$$\frac{z^{p}-1}{z-1}=0\,;$$

supprimons ces racines étrangères par division : l'équation de division devient finalement

$$f(z)=\frac{z^{p^2}-1}{z^{p}-1}=0,$$

ou bien

$$z^{p(p-1)}+z^{p(p-2)}+\cdots+z^{p}+1=0.$$

La substitution $z=x+1$ la transforme en

$$(x+1)^{p(p-1)}+(x+1)^{p(p-2)}+\cdots+(x+1)^{p}+1=0.$$

Le nombre des termes étant p, le terme indépendant de x, après développement, sera égal à p, et la somme aura évidemment la forme

$$x^{p(p-1)}+p\chi(x),$$

$\chi(x)$ étant un polynome entier à coefficients entiers dont le terme indépendant vaut 1. Or, nous venons de montrer que cette somme est en général irréductible. Par conséquent la nouvelle équation de division est aussi irréductible.

Le degré de cette équation est $p(p-1)$. D'autre part une équation irréductible n'est résoluble par radicaux carrés que lorsque son degré est une puissance de 2 ; donc un cercle n'est divisible en p^2 parties égales, avec la règle et le compas, que lorsque $p=2$; bien entendu on suppose que p est un nombre premier.

Il en est de même, nous l'avons déjà remarqué, pour la division en p^α parties égales quand $\alpha>2$.

CHAPITRE IV

La construction du polygone régulier de 17 côtés.

1. Nous venons de voir que la division du cercle en parties égales, au moyen de la règle et du compas, n'est possible que pour les nombres premiers signalés par Gauss. Il y a maintenant intérêt à savoir comment la construction peut réellement être exécutée.

Ce chapitre aura pour objet l'exposition élémentaire de la méthode en s'attachant en particulier au cas du polygone régulier de 17 côtés.

Il n'existe pas encore de construction résultant de considérations purement géométriques ; nous sommes donc obligés de reprendre la voie indiquée par les considérations générales. D'après cela il nous faut considérer tout d'abord les racines de l'équation de division

$$x^{16} + x^{15} + \ldots + x^2 + x + 1 = 0,$$

et construire géométriquement l'expression formée de radicaux carrés que nous en déduirons.

On sait que ces racines peuvent se mettre sous la forme

$$\varepsilon_k = \cos\frac{2k\pi}{17} + i\sin\frac{2k\pi}{17}\ (k = 1, 2, \ldots, 16)\ ;$$

en posant

$$\varepsilon_1 = \cos\frac{2\pi}{17} + i\sin\frac{2\pi}{17},$$

il vient

$$\varepsilon_k = \varepsilon_1^k.$$

Géométriquement ces racines sont représentées dans le plan de la variable imaginaire par les sommets d'un polygone régulier de 17 côtés, inscrit dans un cercle de rayon 1 ayant l'origine pour centre, en laissant de côté le point

origine de la division. Il est indifférent de mettre en évidence la racine ε_1 plutôt qu'une autre ; ce n'est que pour la construction qu'il est nécessaire de préciser la question et d'indiquer quel ε sert de point de départ.

Une fois ε_1 déterminé, l'angle correspondant à ε_k est égal à k fois celui qui correspond à ε_1, ce qui détermine entièrement ε_k.

2. L'idée fondamentale de la solution est la suivante :

En se servant d'une racine primitive par rapport au module 17, on peut ranger les 16 racines de l'équation dans un ordre déterminé de manière à former un cycle.

Comme nous l'avons dit antérieurement, un nombre a est dit racine primitive par rapport à 17, lorsque la congruence

$$a^x \equiv +1 \qquad (\text{mod. } 17)$$

a pour plus petite solution

$$x = 17 - 1 = 16.$$

Le nombre 3 possède cette propriété. On a en effet

$$\left.\begin{array}{llll} 3^1 \equiv 3 & 3^5 \equiv 5 & 3^9 \equiv 14 & 3^{13} \equiv 12 \\ 3^2 \equiv 9 & 3^6 \equiv 15 & 3^{10} \equiv 8 & 3^{14} \equiv 2 \\ 3^3 \equiv 10 & 3^7 \equiv 11 & 3^{11} \equiv 7 & 3^{15} \equiv 6 \\ 3^4 \equiv 13 & 3^8 \equiv 16 & 3^{12} \equiv 4 & 3^{16} \equiv 1 \end{array}\right\} \text{mod. } 17.$$

Rangeons alors les 16 racines dans un ordre tel que leurs indices soient précisément égaux aux restes précédents :

(1) $\varepsilon_3,\ \varepsilon_9,\ \varepsilon_{10},\ \varepsilon_{13},\ \varepsilon_5,\ \varepsilon_{15},\ \varepsilon_{11},\ \varepsilon_{16},\ \varepsilon_{14},\ \varepsilon_8,\ \varepsilon_7,\ \varepsilon_4,\ \varepsilon_{12},\ \varepsilon_2,\ \varepsilon_6,\ \varepsilon_1.$

Remarquons que si r est le reste de 3^λ, on a

$$3^\lambda = 17q + r,$$

donc

$$\varepsilon_r = \varepsilon_1^r = \varepsilon_1^{3^\lambda}.$$

Si r' est le reste qui suit r, on a de même

$$\varepsilon_{r'} = \varepsilon_1^{3^{\lambda+1}} = (\varepsilon_1^{3^\lambda})^3 = \varepsilon_r^3.$$

Donc dans la suite des racines, chaque racine est le cube de la précédente.

La méthode de Gauss consiste à décomposer ce cycle en sommes contenant respectivement 8, 4, 2, 1 racines correspondant aux diviseurs du nombre 16. Chacune de ces sommes s'appelle une *période* ; les périodes ainsi obtenues peuvent se calculer successivement comme racines de certaines équations du second degré.

Le procédé que nous venons d'esquisser n'est qu'un cas particulier de celui qu'on emploie dans le cas général de la division en p parties égales. Les $p-1$ racines de l'équation de division sont rangées cycliquement à l'aide d'une racine primitive de p ; on en forme des périodes qui se calculent comme racines de certaines équations auxiliaires (*). Le degré de ces dernières dépend des facteurs premiers de $p-1$; ce ne sont donc pas nécessairement des équations du 2ᵉ degré.

Le cas général a été traité en détail par Gauss dans ses « *Disquisitiones* », et aussi par Bachmann, dans son opuscule « *Théorie de la division du cercle en parties égales* » (Leipzig, 1872).

3. La formation des périodes se fait de la manière suivante. On forme deux périodes de 8 racines en prenant dans le cycle (1) les racines de rang pair, puis celles de rang impair. Désignons ces périodes par x_1 et x_2 ; remplaçons pour abréger chaque racine par son indice, nous écrirons symboliquement

$$x_1 = 9 + 13 + 15 + 16 + 8 + 4 + 2 + 1,$$
$$x_2 = 3 + 10 + 5 + 11 + 14 + 7 + 12 + 6.$$

Opérons sur x_1 et x_2 de la même manière ; nous formerons 4 périodes à 4 termes :

(*) Voir la Trigonométrie de Briot et Bouquet. — Propriétés des racines de l'équation binome. J. G.

$$y_1 = 13 + 16 + 4 + 1,$$
$$y_2 = 9 + 15 + 8 + 2,$$
$$y_3 = 10 + 11 + 7 + 6,$$
$$y_4 = 3 + 5 + 14 + 12.$$

Opérant enfin de même sur les y ; nous obtenons 8 périodes à 2 termes :

$$z_1 = 16 + 1, \qquad z_5 = 11 + 6,$$
$$z_2 = 13 + 4, \qquad z_6 = 10 + 7,$$
$$z_3 = 15 + 2, \qquad z_7 = 5 + 12,$$
$$z_4 = 9 + 8, \qquad z_8 = 3 + 14.$$

Il s'agit maintenant de montrer que ces diverses périodes peuvent se calculer à l'aide de racines carrées.

4. Le simple aspect de ce dernier tableau montre que la somme des restes correspondant aux racines formant une période z est toujours égale à 17 (*). Ces racines sont donc ε_r et ε_{17-r},

$$\varepsilon_r = \cos r\frac{2\pi}{17} + i \sin r\frac{2\pi}{17},$$

$$\varepsilon_{r'} = \varepsilon_{17-r} = \cos(17 - r)\frac{2\pi}{17} + i \sin(17 - r)\frac{2\pi}{17}$$

$$= \cos r\frac{2\pi}{17} - i \sin r\frac{2\pi}{17} ;$$

donc

$$\varepsilon_r + \varepsilon_{r'} = 2 \cos r\frac{2\pi}{17}.$$

Toutes les périodes z sont donc réelles. Il vient par suite

(*) On peut le démontrer de la manière suivante :

Si on remonte des périodes z aux y, aux x, puis au cycle (1), cela revient à insérer entre les deux racines qui forment un z successivement 1, 3, 5, 7 termes. Si donc une de ces racines correspond au reste r fourni par 3^k, l'autre correspondra à un reste r' fourni par 3^{k+8}. Donc

$$r + r' \equiv 3^k + 3^{k+8} \ (\text{mod. } 17) \equiv 3^k(1 + 3^8) \equiv 17.3^k.$$

Cette somme est donc divisible par 17, et comme r et r' sont inférieurs à 17 il en résulte $r + r' = 17$. J. G.

$$z_1 = 2\cos\frac{2\pi}{17}, \qquad z_5 = 2\cos 6\,\frac{2\pi}{17},$$

$$z_2 = 2\cos 4\,\frac{2\pi}{17}, \qquad z_6 = 2\cos 7\,\frac{2\pi}{17},$$

$$z_3 = 2\cos 2\,\frac{2\pi}{17}, \qquad z_7 = 2\cos 5\,\frac{2\pi}{17},$$

$$z_4 = 2\cos 8\,\frac{2\pi}{17}, \qquad z_8 = 2\cos 3\,\frac{2\pi}{17}.$$

On a d'ailleurs, par définition,

$$x_1 = z_1 + z_2 + z_3 + z_4, \qquad x_2 = z_5 + z_6 + z_7 + z_8,$$

$$y_1 = z_1 + z_2, \quad y_2 = z_3 + z_4, \quad y_3 = z_5 + z_6, \quad y_4 = z_7 + z_8.$$

5. Il nous sera nécessaire de connaître la grandeur relative des différentes périodes. A cet effet nous emploierons l'artifice suivant. Divisons la moitié du cercle de rayon 1 en 17 parties égales (*fig.* 3), et désignons les distances du premier point de division O aux suivants $A_1, A_2, \ldots\ldots A_{17}$ par

$$S_1, S_2, \ldots\ldots, S_{17},$$

S_{17} étant égal au diamètre, c'est-à-dire égal à 2.

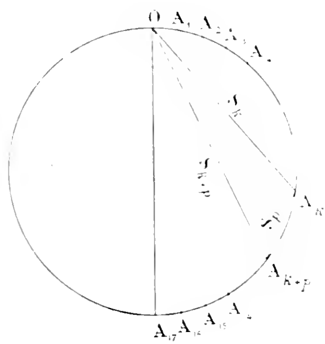


Fig. 3

L'angle $OA_{17}A_k$ a même mesure que la moitié de l'arc OA_k, lequel vaut $\frac{2k\pi}{34}$; on a donc

$$S_k = 2\sin\frac{k\pi}{34} = 2\cos\frac{(17-k)\pi}{34}.$$

Pour que cette formule soit identique à $2\cos h\,\frac{2\pi}{17}$, il faut que

$$4h = 17 - k,$$

$$k = 17 - 4h.$$

En donnant à h les valeurs 1, 2, 3, 4, 5, 6, 7, 8, on trouve pour k les valeurs

$$13, \quad 9, \quad 5, \quad 1, \quad -3, \quad -7, \quad -11, \quad -15.$$

Donc

$$z_1 = S_{13}, \qquad z_5 = -S_7,$$
$$z_2 = S_1, \qquad z_6 = -S_{11},$$
$$z_3 = S_9, \qquad z_7 = -S_3,$$
$$z_4 = -S_{15}, \qquad z_8 = S_5.$$

La figure montre que S_k croît avec l'indice ; donc l'ordre de grandeur croissante des périodes z est

$$z_4, \quad z_6, \quad z_5, \quad z_7, \quad z_2, \quad z_8, \quad z_3, \quad z_1.$$

D'autre part la corde $A_k A_{k+p}$ sous-tend p divisions de la demi-circonférence et vaut S_p ; le triangle OA_kA_{k+p} montre alors que

$$S_{k+p} < S_k + S_p$$

et *a fortiori*

$$S_{k+p} < S_{k+r} + S_{p+r}.$$

Si on calcule alors les différences deux à deux des périodes y, on trouve aisément

$$y_1 - y_2 = S_{13} + S_1 - S_9 + S_{15} > 0,$$
$$y_1 - y_3 = S_{13} + S_1 + S_7 + S_{11} > 0,$$
$$y_1 - y_4 = S_{13} + S_1 + S_3 - S_5 > 0,$$
$$y_2 - y_3 = S_9 - S_{15} + S_7 + S_{11} > 0,$$
$$y_2 - y_4 = S_9 - S_{15} + S_3 - S_5 < 0,$$
$$y_3 - y_4 = -S_7 - S_{11} - S_{13} - S_5 < 0.$$

Donc

$$y_3 < y_2 < y_4 < y_1.$$

Enfin on voit de même que

$$x_2 < x_1.$$

6. Nous nous proposons maintenant de calculer $z_1 = 2\cos\frac{2\pi}{17}$. Ce calcul fait et cette quantité construite, il sera aisé d'en déduire le côté du polygone régulier de 17 côtés.

Associons z_1 à la période z_2 qui forme avec elle la période y_1 ; on a d'abord

$$z_1 + z_2 = y_1.$$

Cherchons maintenant à calculer $z_1 z_2$.

$$z_1 z_2 = (16 + 1)(13 + 4) ;$$

dans ce calcul symbolique, le produit kp représente en réalité

$$\varepsilon_k . \varepsilon_p = \varepsilon_{k+p} ;$$

par conséquent il doit se représenter symboliquement par $k + p$, en ayant bien entendu soin de retrancher 17 de $k + p$ chaque fois qu'on le peut. Il vient ainsi

$$z_1 z_2 = 12 + 3 + 14 + 5 = y_4.$$

Donc z_1 et z_2 sont les racines de l'équation du 2e degré

$$(\zeta) \qquad z^2 - y_1 z + y_4 = 0,$$

d'où, puisque $z_1 > z_2$,

$$z_1 = \frac{y_1 + \sqrt{y_1^2 - 4y_4}}{2}, \qquad z_2 = \frac{y_1 - \sqrt{y_1^2 - 4y_4}}{2}.$$

Il faut donc connaître y_1 et y_4. Pour cela associons à y_1 la période y_2 qui forme avec elle la période x_1 et à y_4 la période y_3 qui forme avec elle la période x_2.

On a d'abord $$y_1 + y_2 = x_1.$$

Puis

$$y_1 y_2 = (13 + 16 + 4 + 1)(9 + 15 + 8 + 2).$$

En effectuant ce produit suivant les règles du calcul symbolique, le second membre devient égal à la somme de toutes les racines, c'est-à-dire à -1.

Donc y_1 et y_2 sont les racines de l'équation

$$(\eta) \qquad y^2 - x_1 y - 1 = 0,$$

d'où

$$y_1 = \frac{x_1 + \sqrt{x_1^2 + 4}}{2},$$

$$y_2 = \frac{x_1 - \sqrt{x_1^2 + 4}}{2}.$$

De même on a

$$y_3 + y_4 = x_2;$$

on vérifierait comme précédemment que

$$y_3 y_4 = -1;$$

donc y_3 et y_4 sont les racines de l'équation

$$(\eta_2) \qquad y^2 - x_2 y - 1 = 0,$$

d'où

$$y_4 = \frac{x_2 + \sqrt{x_2^2 - 4}}{2},$$

$$y_3 = \frac{x_2 - \sqrt{x_2^2 - 4}}{2},$$

puisque $y_3 < y_4$.

Reste enfin à calculer x_1 et x_2. Or $x_1 + x_2$ est égal à la somme de toutes les racines, c'est-à-dire à -1. En faisant le produit $x_1 x_2$ d'après les règles du calcul symbolique, on trouve que ce produit contient 64 termes et qu'il est égal à 4 fois la somme de toutes les racines, c'est-à-dire à -4 ; de sorte que x_1 et x_2 sont racines de l'équation

$$(\xi) \qquad x^2 + x - 4 = 0,$$

d'où

$$x_1 = \frac{-1 + \sqrt{17}}{2}, \qquad x_2 = \frac{-1 - \sqrt{17}}{2},$$

puisque $x_1 > x_2$.

En résolvant successivement les équations ξ, η_1, η_2, ζ, z_1 se calcule bien par une suite de racines carrées.

En faisant ce calcul, on voit que z_1 dépend des quatre radicaux

$$\sqrt{17}, \qquad \sqrt{x_1^2 + 4}, \qquad \sqrt{x_2^2 - 4}, \qquad \sqrt{y_1^2 - 4y_2}.$$

Si donc on veut mettre z_1 sous la forme normale, il faut voir si l'un de ces radicaux ne s'exprime pas rationnellement en fonction des autres. Or

$$\sqrt{x_1^2 + 4} = y_1 - y_2,$$

$$\sqrt{x_2^2 - 4} = y_4 - y_3.$$

En calculant symboliquement, on vérifie que

$$(y_1 - y_2)(y_3 - y_4) = 2(x_1 - x_2),$$

c'est-à-dire

$$\sqrt{x_1^2 + 4}\sqrt{x_2^2 + 4} = 2\sqrt{17}.$$

Cette égalité montre que si des trois différences $y_1 - y_2$, $y_3 - y_4$, $x_1 - x_2$, deux sont positives, il en est de même de la troisième, ce qui est conforme aux résultats obtenus directement.

Remplaçons maintenant x_1, y_1, y_3 par leurs valeurs numériques ; on trouve successivement

$$x_1 = \frac{-1 + \sqrt{17}}{2},$$

$$y_1 = \frac{-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}}}{4},$$

$$y_3 = \frac{-1 - \sqrt{17} + \sqrt{34 + 2\sqrt{17}}}{4},$$

$$z_1 = \frac{-1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}}}{8}$$
$$+ \frac{\sqrt{68 + 12\sqrt{17} - 16\sqrt{34 + 2\sqrt{17}} - 2(1 - \sqrt{17})\sqrt{34 - 2\sqrt{17}}}}{8}.$$

La partie algébrique de notre problème est donc terminée. Nous avons déjà fait la remarque qu'on ne connaît pas de construction du polygone régulier de 17 côtés déduite de considérations purement géométriques ; il s'agit donc maintenant de construire nos expressions algébriques, c'est-à-dire les racines de nos équations du second degré.

7. Qu'il me soit permis d'intercaler ici une digression historique sur les constructions avec la règle et le compas.

Dans la géométrie des Anciens, l'usage de la règle et du compas est toujours simultané ; l'art consiste à rapprocher les différentes parties de la figure de telle manière qu'on n'ait à dessiner aucune ligne inutile. Il est indifférent que

les constructions successives se fassent avec la règle ou le compas.

Par contre, en 1797, l'Italien Mascheroni a fait la tentative, couronnée de succès, d'exécuter toutes les constructions avec le compas seul ; il a exposé ses procédés dans sa « *Geometria del compasso* », et prétend que les constructions au compas sont plus exactes que celles avec la règle. Ainsi qu'il le dit expressément, il écrit pour les arts mécaniques ; il a donc toujours un but pratique devant les yeux. L'ouvrage original de Mascheroni est difficile à lire, et nous devons remercier M. Hutt d'en avoir donné un petit résumé en allemand « *Les Constructions de Mascheroni* » (Halle, 1880).

Bientôt après, les géomètres français, en particulier les disciples de Carnot, l'auteur de la *Géométrie de position*, ont essayé inversement d'exécuter toutes les constructions autant que possible avec la règle (Voir aussi Lambert, Perspective libre, 1774).

Ici se pose une question, à laquelle l'Algèbre permet de répondre immédiatement : Dans quel cas la solution d'un problème d'Algèbre peut-elle se construire avec la règle seule ? Les auteurs cités n'ont pas donné de réponse bien catégorique. Nous dirons :

La règle permet de construire toutes les expressions algébriques dont la forme est rationnelle.

Dans le même ordre d'idées, Brianchon publia en 1818 un petit écrit « *Les applications de la théorie des transversales* » dans lequel il montra que dans beaucoup de cas on peut se tirer d'affaire avec la règle seule. Il insiste de son côté sur la valeur pratique de ses méthodes, qui sont destinées à faciliter les opérations du géomètre-topographe.

C'est Poncelet qui, le premier, dans son « *Traité des propriétés projectives* » (Vol. I, 351-357) a émis cette idée qu'il suffit de tracer dans le plan un seul cercle fixe pour pouvoir construire à l'aide de la règle toutes les

expressions dépendant de radicaux carrés. Il faut connaître d'ailleurs le centre de ce cercle.

Cette idée a été développée par Steiner (1833) dans un écrit célèbre, intitulé : *Les constructions géométriques exécutées à l'aide de la règle et d'un cercle fixe*.

8. Pour effectuer la construction du polygone régulier de 17 côtés, nous suivrons la méthode indiquée par von Staudt (Journal de Crelle, T. 24, 1842), modifiée plus tard par Schrœter (Journal de Crelle, T. 75, 1872). La construction du polygone de 17 côtés y est faite selon les règles indiquées par Poncelet et Steiner; on s'y sert de la règle et d'un cercle fixe.

Montrons d'abord comment, à l'aide de la règle et d'un cercle fixe, dont le rayon est égal à l'unité, on peut construire les racines d'une équation du second degré,

$$x^2 - px + q = 0,$$

dont les racines sont x_1 et x_2 (*).

Menons (*fig.* 4) un diamètre AB du cercle fixe et les tangentes à ses deux extrémités; adoptons sur ces tangentes une direction positive. Portons sur la tangente supérieure un segment $\overline{AD}$ mesuré par $\frac{4}{p}$; sur la tangente inférieure un segment $\overline{BC}$ mesuré par $\frac{q}{p}$; joignons C et D, et marquons les points M_1 et M_2 où la droite CD rencontre le cercle; menons enfin les droites AM_1 et AM_2 qui rencontrent la tangente inférieure en X_1 et X_2; les deux segments $\overline{BX_1}$, $\overline{BX_2}$ ont pour mesures x_1 et x_2.

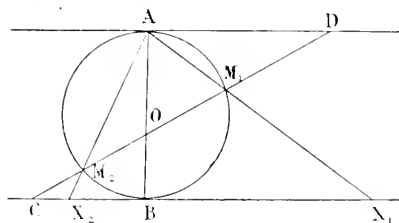


Fig. 4

(*) On ne fait aucune hypothèse sur le signe des racines.

En effet, supposons que

$$\overline{BX_1} = x_1, \qquad \overline{BX_2} = x_2,$$
$$x_1 + x_2 = p, \qquad x_1 x_2 = q.$$

La tangente en B peut être considérée comme la figure inverse du cercle O, le centre d'inversion étant A et la puissance d'inversion $\overline{AB}^2$. Donc

$$\overline{AM_1}.\overline{AX_1} = \overline{AM_2}.\overline{AX_2} = \overline{AB}^2,$$

ce qui prouve que les quatre points M_1, M_2, X_1, X_2 sont sur un même cercle. Il en résulte

$$\overline{CX_1}.\overline{CX_2} = \overline{CM_1}.\overline{CM_2} = \overline{CB}^2$$

ou bien

$$(\overline{BX_1} - \overline{BC})(\overline{BX_2} - \overline{BC}) = \overline{BC}^2, \text{ (*)}$$

d'où

$$\overline{BC} = \frac{\overline{BX_1}.\overline{BX_2}}{\overline{BX_1} + \overline{BX_2}} = \frac{x_1 x_2}{x_1 + x_2} = \frac{q}{p}.$$

Les triangles semblables ADM_1, X_1M_1C nous donnent en grandeur et en signe, à condition d'écrire les sommets homologues aux mêmes places,

$$\frac{\overline{AD}}{\overline{X_1C}} = \frac{\overline{AM_1}}{\overline{X_1M_1}} = \frac{\overline{AM_1}.\overline{AX_1}}{\overline{X_1M_1}.\overline{AX_1}}.$$

Or $\overline{AM_1}.\overline{AX_1} = \overline{AB}^2$; le produit

$$\overline{X_1M_1}.\overline{AX_1} = -\overline{X_1M_1}.\overline{X_1A} = -\overline{BX_1}^2 ;$$
$$\overline{X_1C} = -\overline{CX_1} ;$$

il vient donc

$$\overline{CX_1} = \frac{\overline{AD}}{\overline{AB}^2} \cdot \overline{BX_1}^2.$$

On aurait de même

$$\overline{CX_2} = \frac{\overline{AD}}{\overline{AB}^2} \cdot \overline{BX_2}^2.$$

(*) D'après la relation générale

$$\overline{PQ} = \overline{OQ} - \overline{OP},$$

si les trois points O, P, Q sont en ligne droite.

Observons que

$$\overline{CX_1} = \overline{BX_1} - \overline{BC}, \qquad \overline{CX_2} = \overline{BX_2} - \overline{BC}.$$

Il vient alors, en retranchant membre à membre et divisant par $\overline{BX_1} - \overline{BX_2}$,

$$1 = \frac{\overline{AD}}{\overline{AB}^2} \cdot (\overline{BX_1} + \overline{BX_2}),$$

d'où

$$\overline{AD} = \frac{\overline{AB}^2}{\overline{BX_1} + \overline{BX_2}} = \frac{4}{x_1 + x_2} = \frac{4}{p}.$$

La règle énoncée est donc justifiée (*).

9. C'est d'après ce procédé que nous allons construire les racines de nos quatre équations du second degré. Ce sont

(ξ)	$x^2+x-4=0$,	ayant pour racines	x_1 et x_2 ;	$x_1>x_2$;
(η)	$y^2-x_1y-1=0$	—	y_1 et y_2 ;	$y_1>y_2$;
(η′)	$y^2-x_2y-1=0$	—	y_3 et y_4 ;	$y_4>y_3$;
(ζ)	$z^2-y_1z+y_4=0$	—	z_1 et z_2 ;	$z_1>z_2$.

Cette dernière donne

$$z_1 = 2\cos\frac{2\pi}{17},$$

d'où il est facile de déduire le polygone régulier de 17 côtés. Remarquons d'ailleurs que pour construire z_1, il suffit de construire x_1, x_2, y_1, y_4.

Il faudra donc porter les segments suivants : sur la tangente en A,

$$-4, \qquad \frac{4}{x_1}, \qquad \frac{4}{x_2}, \qquad \frac{4}{y_1};$$

sur la tangente en B,

$$+4, \qquad -\frac{1}{x_1}, \qquad -\frac{1}{x_2}, \qquad \frac{y_4}{y_1}.$$

(*) Remarquons que cette construction suppose qu'on a tracé au préalable les tangentes aux deux extrémités du diamètre AB.

Deux remarques préliminaires vont nous être utiles (*fig.* 5) :

1° Joignons un point M du cercle aux points A et B et marquons les points C et D où ces droites rencontrent respectivement les tangentes en B et A. Il est clair que BC et AD seront de même sens. De plus les triangles rectangles ABC, ABD sont évidemment semblables et donnent

Fig. 5

$$\frac{AD}{AB} = \frac{AB}{BC} \qquad \text{ou} \qquad AD.BC = \overline{AB}^2.$$

donc aussi

$$\overline{AD}.\overline{BC} = \overline{AB}^2 = 4.$$

Donc
$$\overline{AD} = \frac{4}{\overline{BC}}.$$

2° Prenons sur AB, entre A et B, un point I tel que

$$\frac{IA}{IB} = 4.$$

Menons la droite DI qui rencontre la tangente en B en E ; il est clair que les segments AD et BE sont de sens opposé et que leur rapport vaut 4.

Donc
$$\frac{\overline{AD}}{\overline{BE}} = -4.$$

$$\overline{BE} = -\frac{\overline{AD}}{4}.$$

Il est maintenant facile de construire les racines des équations successives.

Construction des racines de l'équation ξ (*fig.* 6). — On porte sur la tangente en A un segment $AD = -4$; sur

la tangente en B le segment $\overline{BC} = +4$; la droite CD rencontre le cercle en deux points que l'on joint au

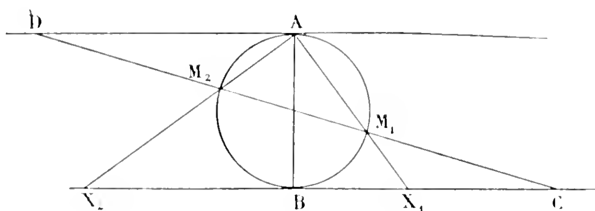


Fig. 6

point A; ces droites rencontrent la tangente en B en deux points X_1 et X_2, tels que

$$\overline{BX_1} = x_1, \qquad \overline{BX_2} = x_2.$$

Construction des racines de l'équation r_1 (*fig.* 7). — Il faut porter sur la tangente en A le segment $\frac{4}{x_1}$. Pour cela (1[re] rem.) on joint X_1 (*) au point A, le point de rencontre M_1 avec le cercle au point B, et on marque le point F où BM_1 rencontre la tangente en A.

$$\overline{AF} = \frac{4}{x_1}.$$

Il faut porter ensuite $-\frac{1}{x_1}$ sur la tangente en B. A cet effet (2° rem.) on mène la droite FI qui rencontre la tangente en B au point G :

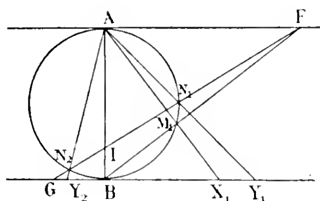


Fig. 7

$$\overline{BG} = -\frac{1}{4}\,\overline{AF} = -\frac{1}{x_1}.$$

Il suffit maintenant de joindre F et G (ce qui est fait), de marquer les points N_1 et N_2 où cette droite rencontre le cercle, de les joindre au point A, de marquer enfin les points Y_1 et Y_2

(*) C'est le point précédemment déterminé.

où ces droites rencontrent la tangente en B.

$$\overline{BY_1} = y_1, \qquad \overline{BY_2} = y_2.$$

Construction des racines de l'équation η' (*fig.* 8). — La solution est la même que précédemment, sauf que X_2 joue le rôle de X_1.

Fig. 8

On mène la droite BM_2 qui rencontre la tangente supérieure en H :

$$\overline{AH} = \frac{1}{x_2}.$$

On tire HI qui rencontre la tangente inférieure en K;

$$\overline{BK} = -\frac{1}{x_2}.$$

On marque les points M_3 et M_4 où cette droite rencontre le cercle ; on les projette du point A sur la tangente en B en Y_3 et Y_4. On a

$$\overline{BY_3} = y_3, \qquad \overline{BY_4} = y_4.$$

On a mis Y_4 à droite parce que $y_4 > y_3$.

Construction des racines de l'équation ζ (*fig.* 9). — Pour porter sur la tangente supérieure $\frac{1}{y_1}$, on mène la droite AY_1 qui rencontre le cercle en X_1. De B on projette X_1 sur la tangente supérieure en L :

$$\overline{AL} = \frac{1}{y_1}.$$

Il s'agit maintenant de porter sur la tangente inférieure $\frac{y_4}{y_1}$. Pour cela on porte $AS = -1$; on tire SY_4 qui rencontre AB en R; on mène ensuite RL qui rencontre la tangente en B en P. On a

Fig. 9

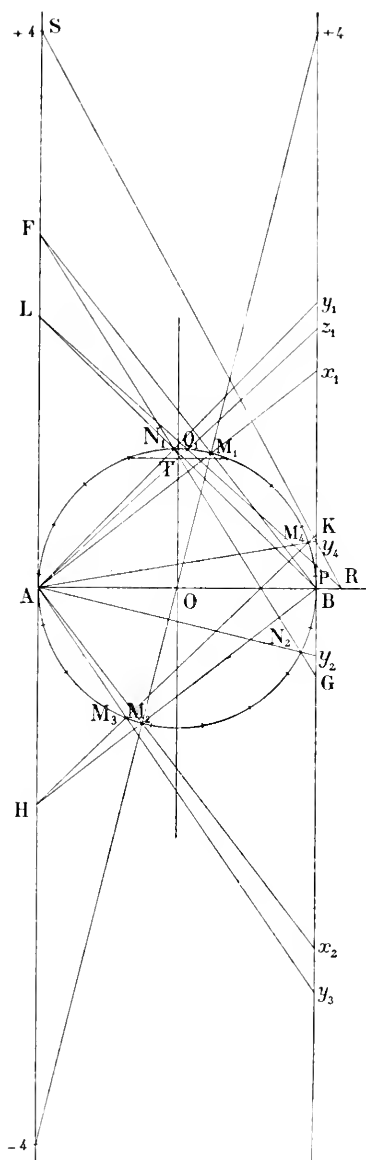


Fig. 10.

$$\frac{BP}{AL} = \frac{RB}{RA} = \frac{BY_4}{AS}.$$

Donc

$$BP = \frac{AL.BY_4}{AS}$$

$$= \frac{\frac{4}{y_1} \cdot y_4}{4} = \frac{y_4}{y_1}.$$

Marquons le point Q_1 le plus à droite où la droite RL rencontre le cercle ; projetons-le du point A en Z_1 sur la tangente en B ; on aura

$$\overline{BZ_1} = z_1 = 2 \cos \frac{2\pi}{17}.$$

On en déduit $\cos \frac{2\pi}{17}$ en menant par O la parallèle OT à la tangente en B. La perpendiculaire élevée en ce point à OT détermine immédiatement le premier et le seizième sommet du polygone de 17 côtés.

La période z_1 a été choisie arbitrairement ; on aurait pu construire de même toute autre période à deux termes, ce qui permettrait de trouver tous les autres cosinus. Ces construc-

tions, faites sur des figures séparées, afin qu'on pût les suivre plus aisément, ont été réunies dans une seule figure ci-contre (*fig.* 10), qui donne la construction complète du polygone régulier de 17 côtés.



CHAPITRE V

Généralités sur les constructions d'expressions algébriques.

1. Nous allons maintenant laisser de côté les constructions avec la règle et le compas. Avant de quitter ce sujet, mentionnons une méthode nouvelle et très simple, pour effectuer certaines constructions : le *pliage du papier*. M. Hermann Wiener a montré comment, en pliant convenablement un papier, on peut obtenir le réseau des polyèdres réguliers (*). Un fait singulier, c'est que, vers la même époque, un mathématicien hindou, Sundara Row, de Madras, a fait paraître un petit écrit sur le même sujet, « On paper folding » (sur le pliage du papier). La même idée y est développée d'une façon plus étendue ; l'auteur montre, par exemple, comment, en pliant convenablement un papier, on peut construire par points des lignes courbes telles que l'ellipse, la cissoïde, etc. (Londres, Macmillan 1893).

2. Cherchons maintenant comment on peut résoudre géométriquement les problèmes dont la forme analytique est une équation du 3e degré ou de degré supérieur, et voyons en particulier comment les géomètres anciens y sont parvenus.

L'idée la plus naturelle est de recourir aux coniques ; les anciens s'en sont beaucoup servis ; ils ont trouvé en particulier que l'emploi de ces courbes permettait de résoudre

---

(*) Voir le catalogue de l'exposition mathématique de Munich 1893, édité par Dyk ; Appendice p. 52.

le problème de la duplication du cube et de la trisection de l'angle.

Voici, en quelques mots, comment on peut résoudre graphiquement l'équation du 3ᵉ degré

$$x^3 + ax^2 + bx + c = 0,$$

ou l'équation du 4ᵉ degré

$$x^4 + ax^3 + bx^2 + cx + d = 0.$$

Posons $x^2 = y$; nos équations deviennent

$$xy + ay + bx + c = 0,$$

et

$$y^2 + axy + by + cx + d = 0.$$

Les racines des équations proposées sont donc les abscisses des points communs à deux coniques.

L'équation $x^2 = y$ représente une parabole dont l'axe est dirigé suivant Oy. La seconde équation

$$xy + ay + bx + c = 0$$

représente (*fig.* 11) une hyperbole dont les asymptotes sont parallèles aux axes de coordonnées. L'un des quatre points d'intersection est à l'infini sur l'axe des y, les trois autres sont à distance finie, et leurs abscisses sont les racines de l'équation du 3ᵉ degré.

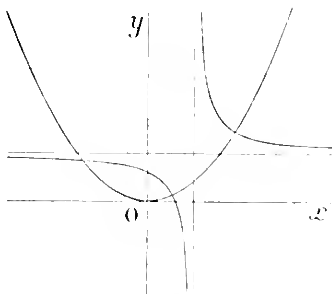


Fig. 11

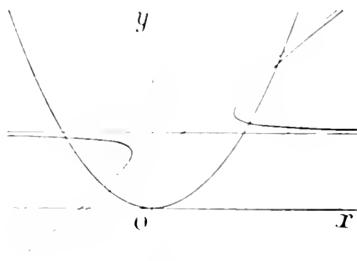


Fig. 12

Dans le 2ᵉ cas, la parabole est la même. L'hyperbole (*fig.* 12) a toujours une asymptote parallèle à Ox, tandis que l'autre n'est plus perpendiculaire à Ox ; les courbes ont maintenant quatre points d'intersection à distance finie.

On trouvera l'exposition détaillée des procédés des géomètres anciens dans le grand ouvrage de M. Maurice Cantor : *Histoire des Mathématiques* (Leipzig 1894, 2e édition). Comme ouvrages intéressants sur le même sujet, on peut encore citer : *Les coniques dans l'antiquité*, par Zeuthen (Copenhague 1886) ; la *Géométrie analytique* de Baltzer (Leipzig 1882).

3. Outre les coniques, les anciens utilisèrent aussi des courbes de degré supérieur, qui furent d'ailleurs précisément inventées à l'occasion des problèmes qui nous occupent. Nous ne parlerons ici que de la *cissoïde* et de la *conchoïde*.

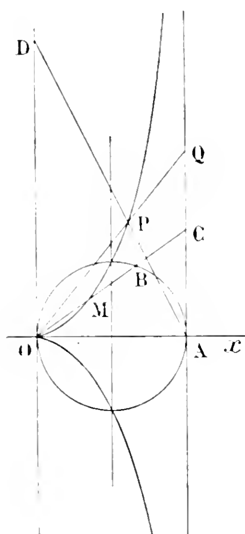


Fig. 13

La *cissoïde de Dioclès* (150 ans av. J.-C.) se construit de la manière suivante. On donne (*fig.* 13) un cercle, un diamètre OA et la tangente en A. Une sécante menée par O rencontre le cercle en B et la tangente en C ; on porte sur cette sécante, à partir de O, une longueur OM = BC. Le lieu géométrique de M, quand on fait tourner la sécante autour de O, est la *cissoïde*.

Formons son équation, en prenant pour axes des x et des y le diamètre OA et la tangente en O. Posons $OM = r$, $\widehat{MOx} = \theta$, et prenons pour unité de longueur le diamètre du cercle. Il vient alors

$$OC = \frac{1}{\cos\theta}, \qquad OB = \cos\theta,$$

donc

$$r = \frac{1}{\cos\theta} - \cos\theta = \frac{\sin^2\theta}{\cos\theta}.$$

D'où, en remarquant que

$$x = r\cos\theta, \qquad y = r\sin\theta,$$

on déduit l'équation

$$(x^2 + y^2)x - y^2 = 0.$$

La courbe est donc du 3e ordre ; elle possède un point de rebroussement à l'origine, et admet l'axe des x comme axe de symétrie. La tangente en A est asymptote à la courbe, laquelle passe en outre par les points cycliques.

Pour résoudre à l'aide de cette courbe le problème de Délos, écrivons son équation sous la forme

$$\left(\frac{y}{x}\right)^3 = \frac{y}{1 - x}.$$

On voit alors que la cissoïde peut être engendrée par l'intersection des deux droites variables

$$\frac{y}{x} = \lambda, \qquad \frac{y}{1 - x} = \lambda^3.$$

La première passe par l'origine et intercepte sur la tangente en A la longueur λ ; la seconde passe par le point A ($x = 1$, $y = 0$) et intercepte sur l'axe des y la longueur λ^3.

De là une construction simple de $\sqrt[3]{2}$. On prend sur Oy une longueur OD $= +2$; on mène AD qui coupe la cissoïde au seul point réel P ; on mène enfin OP qui détermine sur la tangente en A la longueur

$$AQ = \sqrt[3]{OD} = \sqrt[3]{2}.$$

4. La *conchoïde de Nicomède* (environ 150 ans av. J.-C.) s'obtient de la manière suivante.

Soit O (*fig.* 14) un point fixe, et a sa distance à une droite fixe D. Faisons tourner autour du point O un rayon mobile ; à partir du point P, où il rencontre la droite, por-

tons sur lui dans les deux sens une même longueur b : le lieu des extrémités de ces longueurs est la conchoïde.

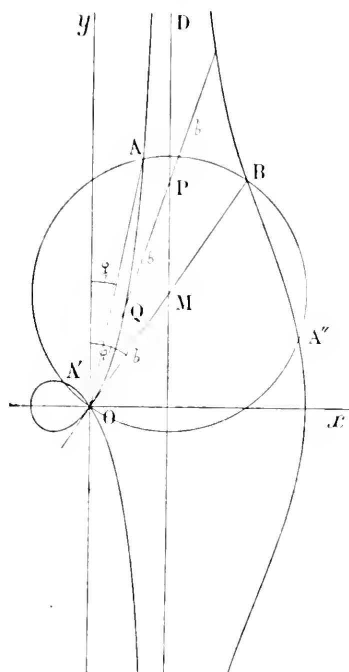


Fig. 14

Selon que b est supérieur ou inférieur à a, elle admet à l'origine un point double ou un point isolé; pour $b = a$, c'est un point de rebroussement.

De cette construction on déduit très simplement l'équation de la ligne en prenant pour axes des x et des y la perpendiculaire et la parallèle menées par O à la droite D.

Posant $OQ = r$, on a

$$\frac{r}{x} = \frac{b}{x - a}.$$

d'où
$$(x^2 + y^2)(x - a)^2 - b^2x^2 = 0.$$

La conchoïde est donc du quatrième ordre, possède un point double à l'origine, se compose de deux branches ayant pour asymptote commune la droite $x = a$. En outre on voit que la courbe passe par les points cycliques, fait important pour la suite des raisonnements.

Voici comment cette courbe, supposée construite, permet d'effectuer la trisection d'un angle quelconque.

Soit $\varphi = MOy$ l'angle à diviser en trois parties égales. Prenons sur le côté OM une longueur $OM = b$, menons par M la parallèle à Oy ; construisons enfin la conchoïde

ayant O comme point double, la parallèle comme asymptote et caractérisée par la longueur b.

Cela fait, décrivons de M comme centre un cercle de rayon b; la figure montre évidemment qu'il rencontre la conchoïde en un point A situé à l'intérieur de l'angle MOy. On démontre sans difficulté aucune que

$$\widehat{AOy} = \frac{1}{3}\widehat{MOy}.$$

Nos recherches précédentes nous ont appris que le problème de la trisection de l'angle est un problème du 3e degré; il admet les trois solutions

$$\frac{\varphi}{3}, \qquad \frac{\varphi + 2\pi}{3}, \qquad \frac{\varphi + 4\pi}{3}.$$

Toute construction géométrique qui résout ce problème à l'aide d'une courbe de degré supérieur, doit fournir naturellement toutes les solutions, sans quoi l'équation du problème ne serait pas irréductible.

Ces solutions résultent en effet de notre figure. Le cercle et la conchoïde se coupent en 8 points (*). Deux d'entre eux sont confondus à l'origine, deux autres avec les points cycliques; aucun d'eux ne peut fournir une solution du problème. Restent donc quatre points d'intersection, de sorte qu'il semble y avoir une solution de trop. Cela tient à ce que, parmi les 4 points, se trouve nécessairement le point B, tel que

$$OMB = 2b,$$

point qu'on peut construire sans le secours de la courbe. Il ne reste donc plus que trois points qui correspondent aux trois racines fournies par la solution algébrique.

5. Dans toutes ces constructions à l'aide de courbes

(*) Deux courbes, l'une de degré m, l'autre de degré p, ont mp points communs.

algébriques de degré supérieur, il faut encore élucider la question de l'exécution pratique. Il faut pour cela un appareil qui trace la courbe d'un trait continu ; une construction par points n'est autre chose au fond qu'une méthode d'approximation. On a construit beaucoup d'appareils de ce genre ; il y en a qui étaient déjà connus des géomètres anciens. Nicomède trouva un dispositif simple pour tracer sa conchoïde ; c'est le plus ancien appareil connu, outre la règle et le compas. (Cf. Cantor, Vol. I, p. 302.)

On trouvera une énumération des appareils construits plus récemment dans le catalogue de Dyk, p. 227-230 et 340 ; et p. 42-43 de l'appendice.

DEUXIÈME PARTIE

LES NOMBRES TRANSCENDANTS ET LA QUADRATURE DU CERCLE

CHAPITRE I

Existence des nombres transcendants. Démonstration de M. Cantor.

1. Représentons comme de coutume les nombres par les points d'un axe des abscisses. Si nous nous bornons aux nombres rationnels, les points correspondants rempliront l'axe des abscisses avec une « *densité parfaite* », c'est-à-dire que dans un intervalle, si petit qu'il soit, il y a une infinité de tels points. Néanmoins, comme les géomètres anciens l'avaient déjà reconnu, l'*ensemble continu* des points de l'axe n'est pas épuisé de cette manière; les nombres irrationnels s'introduisent entre les nombres rationnels, et la question se pose si, parmi les nombres irrationnels, il ne faut pas encore faire certaines différences.

Définissons d'abord ce qu'on entend par *nombres algébriques*. On appelle ainsi toute racine d'une équation algébrique

$$a_0\omega^n + a_1\omega^{n-1} + \cdots + a_{n-1}\omega + a_n = 0,$$

dont les coefficients sont des nombres entiers, premiers entre eux. Bien entendu il n'est question que de racines réelles.

Les nombres rationnels en sont un cas particulier comme

racines des équations de la forme

$$a_0\omega + a_1 = 0.$$

Les nombres algébriques réels forment-ils un ensemble continu, ou bien une suite discontinue, telle qu'on puisse insérer d'autres nombres dans ses intervalles? Ces nouveaux nombres, les nombres *transcendants*, seraient alors caractérisés par cette propriété de ne pouvoir être racines d'une équation algébrique entière à coefficients entiers.

Cette question a d'abord été résolue par Liouville (Comptes Rendus 1844, et Journal de Liouville, V. 16, 1851) : il a en effet démontré l'existence de nombres transcendants. Mais sa démonstration, qui s'appuie sur la théorie des fractions continues, est assez compliquée. La question devient beaucoup plus simple lorsqu'on se place au point de vue développé par M. Georges Cantor dans un mémoire d'une importance capitale : *Sur une propriété de l'ensemble des nombres algébriques réels* (Journal de Crelle, t. 77, 1873). Nous allons exposer sa démonstration, en utilisant une idée un peu plus simple, que M. Cantor, sous une forme différente il est vrai, avait signalée à l'assemblée des « Naturforscher » à Halle en 1891.

2. La démonstration repose sur cette propriété que les nombres algébriques forment un ensemble *énumérable*, tandis qu'il en est autrement des nombres transcendants. M. Cantor veut dire par là qu'on peut ranger les premiers dans un certain ordre, tel que chacun d'eux occupe une place déterminée, numérotée pour ainsi dire. Cette proposition peut aussi s'énoncer de la manière suivante :

On peut établir une correspondance univoque entre la multiplicité des nombres algébriques réels et la multiplicité des nombres entiers positifs.

Il semble qu'il y ait là une impossibilité. Les nombres entiers positifs ne forment qu'une partie des nombres

algébriques réels; puisqu'à chaque nombre du premier ensemble on peut faire correspondre un nombre et un seul du second, la partie serait donc égale au tout. Cette objection repose sur une analogie inexacte. Le théorème qui dit que la partie est plus petite que le tout, n'est plus valable quand il s'agit de grandeurs en nombre infini. Il est bien évident par exemple qu'on peut établir une correspondance univoque entre les nombres entiers positifs et les nombres pairs positifs, il suffit d'écrire

$$\begin{matrix} 0 & 1 & 2 & 3 & \ldots & n & \ldots \\ 0 & 2 & 4 & 6 & \ldots & 2n & \ldots \end{matrix}$$

Quand il s'agit de quantités infinies, les mots *grand* et *petit* ne sont pas bien à leur place.

M. Cantor a proposé de les caractériser par leur *puissance* : *Deux collections infinies ont même puissance, lorsqu'on peut établir entre leurs éléments une correspondance univoque.*

Le théorème que nous avons à démontrer prend alors la forme suivante :

L'ensemble des nombres algébriques réels a même puissance que l'ensemble des nombres entiers positifs.

On obtient l'ensemble des nombres algébriques réels en cherchant les racines de toutes les équations algébriques de la forme

$$a_0\omega^n + a_1\omega^{n-1} + \ldots + a_{n-1}\omega + a_n = 0.$$

Tous les a sont supposés premiers entre eux, a_0 est positif et l'équation est irréductible.

Afin de ranger les nombres ainsi obtenus dans un certain ordre, nous considérons leur *hauteur* N, qui est représentée par

$$N = n - 1 + |a_0| + |a_1| + \ldots + |a_n|;$$

$|a_i|$ représente la valeur absolue de a_i. A un nombre donné N correspond un nombre fini d'équations algébriques. En effet, N étant donné, le nombre n a certainement une limite supérieure, puisque N est égal à $n - 1$, aug-

menté de nombres positifs ; en outre la différence $N - n - 1$ est une somme de nombres positifs premiers entre eux, dont le nombre est évidemment fini.

N	n	$\|a_0\|$	$\|a_1\|$	$\|a_2\|$	$\|a_3\|$	$\|a_4\|$	Equation	φN	Racines
1	1	1	0				$x = 0$	1	0
	2	0	0	0			—		
2	1	2	0				—	2	-1
		1	1				$x \pm 1 = 0$		$+1$
	2	1	0	0			—		
3	1	3	0				—	4	-2
		2	1				$2x \pm 1 = 0$		$-\frac{1}{2}$
		1	2				$x \pm 2 = 0$		$+\frac{1}{2}$
	2	2	0	0			—		$+2$
		1	1	0			—		
		1	0	1			—		
	3	1	0	0	0		—		
4	1	4	0				—	12	-3
		3	1				$3x \pm 1 = 0$		$-1,61803$
		2	2				—		$-1,41421$
		1	3				$x \pm 3 = 0$		$-0,70711$
	2	3	0	0			—		$-0,61803$
		2	1	0			—		$-0,33333$
		2	0	1			$2x^2 - 1 = 0$		$+0,33333$
		1	2	0			—		$+0,61803$
		1	1	1			$x^2 \pm x - 1 = 0$		$+0,70711$
		1	0	2			$x^2 - 2 = 0$		$+1,41421$
	3	2	0	0	0		—		$+1,61803$
		1	1	0	0		—		$+3$
		1	0	1	0		—		
		1	0	0	1		—		
	4	1	0	0	0	0	—		

Parmi ces équations, il faut écarter celles qui sont réductibles, ce qui n'offre théoriquement aucune difficulté.

Le nombre des équations correspondant à une valeur donnée de N étant limité, il ne correspond à cette valeur qu'un nombre limité de nombres algébriques. Nous désignerons ce nombre par $\varphi(N)$. Le tableau ci-contre contient le calcul de $\varphi(1)$, $\varphi(2)$, $\varphi(3)$, $\varphi(4)$ et des nombres ω qui leur correspondent.

Rangeons maintenant ces nombres algébriques suivant leur hauteur N, en ordonnant les nombres qui correspondent à une même valeur de N suivant leur grandeur croissante. Nous aurons ainsi tous les nombres algébriques, chacun d'eux à une place déterminée. C'est ce qui a été fait dans le tableau précédent.

Notre proposition est donc démontrée.

3. Voici maintenant la proposition générale que nous avons en vue :

Si on considère une portion de l'axe des x, aussi petite que l'on veut, il s'y trouve une infinité de points qui n'appartiennent certainement pas à un ensemble énumérable donné.

En d'autres termes :

L'ensemble continu des valeurs numériques représentées par les points de l'axe des x contenus dans une portion de cet axe, si petite qu'elle soit, a une puissance plus grande que celle d'un ensemble énumérable donné.

Cela revient visiblement à affirmer l'existence des nombres transcendants ; il suffit de prendre comme ensemble énumérable celui des nombres algébriques.

Pour démontrer ce théorème, dressons le tableau des nombres algébriques, comme précédemment, et écrivons-y tous les nombres sous forme de nombres décimaux ; aucun d'eux ne sera terminé par une suite indéfinie de 9 ; car l'égalité

$$1 = 0{,}999\ldots\ldots$$

montre qu'un tel nombre est un nombre décimal exact.

Si maintenant nous pouvions construire un nombre décimal qui ne soit pas terminé par une suite indéfinie de 9, et qui ne se trouve pas dans notre table, ce serait certainement un nombre transcendant. Un procédé très simple, indiqué par M. G. Cantor, permet de trouver non seulement un tel nombre, mais une infinité, même si les limites entre lesquelles doit se trouver le nombre sont extrêmement rapprochées. Supposons, par exemple, que les cinq premières décimales du nombre soient données (*). Le procédé de M. Cantor est alors le suivant.

On prend pour 6ᵉ décimale un nombre différent de 9 et de la 6ᵉ décimale du *premier* nombre algébrique ; pour 7ᵉ décimale, un nombre différent de 9 et de la 7ᵉ décimale du *second* nombre algébrique, etc. De cette manière, on obtient une fraction décimale indéfinie, qui ne sera pas terminée par une suite indéfinie de 9, et qui certainement n'est pas contenue dans notre table. La proposition est donc démontrée.

On voit aussi par là (si on veut bien nous permettre cette expression) qu'il y a beaucoup plus de nombres transcendants que de nombres algébriques. En effet, quand on détermine les décimales inconnues, on peut choisir, en évitant les 9, huit nombres différents ; on forme ainsi des nombres transcendants au nombre de ∞^{∞}, même quand ils doivent être compris entre des limites aussi rapprochées que l'on veut.

(*) C'est-à-dire que les limites entre lesquelles doit être compris le nombre diffèrent de $\frac{1}{10^5}$.

CHAPITRE II

Coup d'œil historique sur les tentatives de calcul et de construction de π.

Nous allons faire voir que le nombre π appartient à la classe des nombres transcendants dont l'existence a été démontrée dans le chapitre précédent. La preuve rigoureuse en a été fournie par Lindemann en 1882 : il a ainsi résolu définitivement un problème qui a préoccupé les mathématiciens depuis quatre mille ans (aussi loin que peut remonter l'histoire) ; c'est celui de la *quadrature du cercle*.

En effet, si π n'est pas un nombre algébrique, il est impossible de le construire avec la règle et le compas ; la quadrature du cercle est donc impossible au sens où l'entendaient les anciens. Il est intéressant de suivre les tentatives faites en vue de la solution de ce problème aux différentes époques de la science, de voir comme on a toujours essayé de nouvelles constructions avec la règle et le compas, comment enfin ces efforts nécessairement infructueux ont exercé l'influence la plus féconde sur les branches les plus diverses des Mathématiques.

Les éléments de la petite revue historique que nous allons faire sont empruntés à un ouvrage très recommandable de M. Rudio : « Archimède, Huygens, Lambert, Legendre. Quatre mémoires sur la mesure du cercle » (Leipzig 1892). Ce livre contient la traduction allemande des recherches des auteurs nommés ci-dessus. Quoique le mode d'exposition s'éloigne beaucoup des idées modernes dont nous allons faire usage, on y trouvera néanmoins des particularités intéressantes, dont on pourra tirer une utilité pratique au point de vue de l'enseignement.

1. Dans les tentatives faites pour déterminer le rapport du diamètre à la circonférence, on peut d'abord distinguer l'*époque empirique*, dans laquelle on cherche à arriver au but par mesure ou estimation directe.

Le document mathématique le plus ancien qui existe, le « *Papyrus Rhind* » (environ 2000 ans avant J.-C.), énonce déjà le problème sous sa forme bien connue : construire un carré équivalent à un cercle donné. L'auteur du papyrus, *Ahmès*, donne la règle suivante : on retranche d'un diamètre une quantité égale à son neuvième ; on construit un carré ayant pour côté la partie restante ; il est équivalent au cercle. On obtient ainsi pour π une valeur pas trop erronée,

$$\pi = \left(\frac{16}{9}\right)^2 = 3,16\ldots$$

Bien moins exacte est la valeur $\pi = 3$, que l'on trouve dans la Bible (1er Livre des Rois, 7, 23 ; 2e livre de la Chronique, 4, 2.)

2. Les Grecs, Archimède en particulier, s'élevèrent au-dessus de ce point de vue empirique. Dans son livre « κύκλου μέτρησις », ce dernier géomètre calcule la surface du cercle au moyen de celle des polygones inscrits et circonscrits, comme on le fait encore aujourd'hui dans l'enseignement élémentaire. Sa méthode resta en usage jusqu'à l'invention du calcul différentiel : elle fut particulièrement développée et rendue pratique par Huygens (mort en 1654), dans son ouvrage « *de magnitudine circuli inventa* ».

De même que la duplication du cube et la trisection de l'angle, les géomètres grecs cherchèrent à effectuer la quadrature du cercle au moyen de courbes de degré supérieur.

Considérons par exemple la courbe

$$y = \text{arc sin } x.$$

Elle se présente sous la forme d'une sinussoïde à axe vertical. Géométriquement, π se présente comme une or-

donnée particulière de cette courbe ; au point de vue de la théorie des fonctions, c'est une valeur particulière de notre fonction transcendante. Appelons appareil transcendant tout appareil qui trace une courbe transcendante; un appareil transcendant qui dessine la sinussoïde nous donnera une construction géométrique de π.

La courbe $y = \text{arc sin } x$ s'appelle dans le langage moderne une *courbe intégrale*, parce qu'on peut la définir par l'intégrale d'une fonction algébrique,

$$y = \int_0^x \frac{dx}{\sqrt{1-x^2}}.$$

Les anciens désignaient ces courbes sous le nom de *quadratrices* ou τετραγωνίζουσα. La plus connue est la quadratrice de Dinostrate (environ 350 ans avant J.-C.) ; elle avait déjà été construite antérieurement par Hippias (420 av. J.-C.), qui s'en servit pour la trisection de l'angle.

Elle se définit géométriquement de la manière suivante (*fig.* 15).

Étant donné un cercle et deux rayons rectangulaires OA et OB, deux mobiles M et L se meuvent d'un mouvement uniforme, l'un sur le rayon OB, l'autre sur l'arc AB. Ils partent au même instant de leurs positions initiales O et A et arrivent simultanément en B. Le point d'intersection P de OL avec la parallèle MP menée par M à OA décrit la quadratrice.

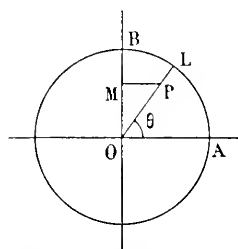


Fig. 15

De cette définition, il résulte que y est proportionnel à θ ; comme d'autre part $y = 1$ pour $\theta = \frac{\pi}{2}$, on a

$$\theta = \frac{\pi}{2} y.$$

De plus

$$\theta = \operatorname{arc\,tg} \frac{y}{x};$$

donc l'équation de la quadratrice est

$$\frac{y}{x} = \operatorname{tg} \frac{\pi y}{2}.$$

Elle rencontre l'axe des x en un point dont l'abscisse est

$$x = \lim \frac{y}{\operatorname{tg} \frac{\pi}{2} y} \quad \text{pour} \quad y = 0;$$

donc

$$x = \frac{2}{\pi}.$$

D'après cette formule, le rayon du cercle est la moyenne proportionnelle entre la longueur du quadrant et l'abscisse du point d'intersection de la quadratrice avec l'axe des x. On peut donc se servir de cette courbe à la fois pour la rectification et la quadrature du cercle. Remarquons d'ailleurs que cela revient simplement à formuler le problème de la rectification sous forme géométrique, aussi longtemps qu'on n'aura pas construit un appareil permettant de décrire la courbe d'un trait continu.

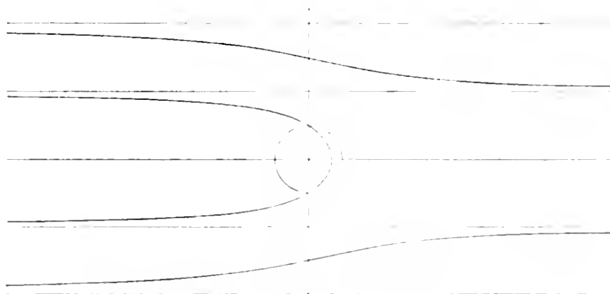


Fig. 16

La figure 16 donne une idée de la forme de la courbe, avec les branches qu'on obtient en considérant les valeurs de θ supérieures à π ou inférieures à $-\pi$. Évidemment

la quadratrice de Dinostrate n'est pas aussi commode que la courbe

$$y = \text{arc sin } x ;$$

mais il ne semble pas que cette dernière ait été utilisée par les géomètres anciens.

3. La période de 1670-1770, caractérisée par les noms de Leibniz, Newton, Euler, est celle de la naissance de l'analyse moderne. Les grandes découvertes se succèdent de près en une suite ininterrompue, et naturellement l'étroite rigueur est quelque peu rejetée à l'arrière-plan. Pour notre point de vue, c'est le développement de la théorie des séries qui est particulièrement important. Un grand nombre de valeurs approchées de π en ont été déduites : qu'il nous suffise de citer la *série de Leibniz* (connue d'ailleurs avant lui) :

$$\frac{\pi}{4} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \ldots$$

Dans cette même période se place la découverte de la dépendance des nombres e et π. Le nombre e, les logarithmes naturels et par suite la fonction exponentielle sont mentionnés d'abord dans les ouvrages de l'Anglais Napier (Neper 1614).

Ce nombre ne semblait d'abord avoir aucun rapport avec les fonctions circulaires et le nombre π, jusqu'à ce qu'Euler eût le courage de considérer des exposants imaginaires ; il arriva de cette manière à la célèbre formule

$$e^{ix} = \cos x + i \sin x,$$

qui, pour $x = \pi$, se réduit à

$$e^{i\pi} = -1 .$$

Cette formule est certainement une des plus remarquables qu'il y ait en Mathématiques. C'est à elle que se rattachent les démonstrations modernes de la transcen-

dance de π ; elles commencent par montrer la transcendance du nombre e.

4. Après 1770 l'esprit critique reprit ses droits. Cette même année parut le livre de Lambert : *Connaissances préliminaires pour ceux qui cherchent la quadrature du cercle*. Il y traite entre autres de l'irrationnalité du nombre π.

En 1794 Legendre démontra définitivement dans ses éléments de Géométrie que π et π^2 sont des nombres irrationnels.

5. Ce n'est que cent ans plus tard que commencent les recherches modernes.

Le point de départ a été le Mémoire de M. Hermite « *Sur la fonction exponentielle* » (Comptes Rendus 1873, publié en 1874). Il y démontre la transcendance du nombre e.

Une démonstration analogue pour π, se rattachant étroitement à celle de M. Hermite, a été donnée par M. Lindemann (Mathematische Annalen, 20, 1882. Voir aussi les Comptes Rendus des académies de Berlin et de Paris).

La question était donc entièrement élucidée pour la première fois ; mais les considérations de MM. Hermite et Lindemann étaient encore très compliquées.

La première simplification a été indiquée par M. Weierstrass dans les « Berliner Berichte » de 1885. Tous les travaux cités précédemment ont été réunis par Bachmann dans son livre : *Leçons sur la nature des nombres irrationnels*, 1892.

Au printemps de 1893 se produisirent de nouvelles et très grandes simplifications. En première ligne il faut citer les mémoires de M. Hilbert dans les « Gœttinger Nachrichten ». Pourtant sa démonstration n'est pas encore absolument élémentaire ; il y reste encore une trace des idées de M. Hermite sous la forme de l'intégrale

$$\int_0^{\infty} z^{\rho} . e^{-z} . dz = \rho\,! \quad (*)$$

Peu de temps après, MM. Hurwitz et Gordan ont montré qu'on peut se passer de cette formule transcendante. (Gœttinger Nachrichten ; Comptes Rendus ; Math. Annalen, Vol. 43).

La démonstration a pris maintenant une forme tout à fait élémentaire et semble accessible à tout le monde. C'est à la marche suivie par M. Gordan que nous rattacherons notre exposé.

(*) $\rho\,! = 1.2.3 \ldots \rho$.

CHAPITRE III

La transcendance du nombre e.

1. Nous nous appuierons sur le développement en série bien connu de e^x :

$$e^x = 1 + \frac{x}{1} + \frac{x^2}{2\,!} + \dots + \frac{x^n}{n\,!} + \dots,$$

convergent pour toutes les valeurs de x.

Insistons, en passant, sur la différence entre la convergence théorique et la convergence pratique. Si on prend $x = 1000$, il est laborieux de calculer e^{1000} au moyen de cette série. Elle est pourtant convergente théoriquement ; on voit facilement qu'à partir du 1000e terme la factorielle $n\,!$ du dénominateur croît plus rapidement que la puissance qui figure au numérateur. Cette circonstance, que $\frac{x^n}{n\,!}$ a pour limite zéro quand n devient infini, est importante pour nos raisonnements ultérieurs.

2. Nous allons démontrer la proposition suivante :

Le nombre e n'est pas un nombre algébrique ; en d'autres termes, ce nombre ne peut être racine d'une équation entière à coefficients entiers

$$F(x) = C_0 + C_1 x + \dots + C_n x^n = 0 ;$$

on peut toujours supposer que les coefficients C_i sont premiers entre eux.

Voici la marche de la démonstration. Nous supposerons qu'il existe un nombre entier n, et des entiers C_i, premiers entre eux, tels que l'on ait

$$F(e) = C_0 + C_1 e + C_2 e^2 + \dots + C_n e^n = 0.$$

En multipliant les deux membres par un certain nombre M, il vient

$$MF(e) = MC_0 + MC_1e + MC_2e^2 + \ldots + MC_ne^n.$$

Nous montrerons qu'on peut choisir ce nombre M de manière à satisfaire aux conditions suivantes :

1° Chacun des produits Me, Me^2, ..., Me^n peut être décomposé en une partie entière M_k et une partie fractionnaire ε_k.

L'identité prend alors la forme

$$MF(e) = MC_0 + M_1C_1 + M_2C_2 + \cdots + M_nC_n$$
$$+ C_1\varepsilon_1 + C_2\varepsilon_2 + \cdots + C_n\varepsilon_n = 0.$$

2° La partie entière

$$MC_0 + M_1C_1 + \ldots + M_nC_n$$

n'est pas nulle. Cela résultera de ce fait que, divisée par un nombre premier, elle donne un reste différent de zéro.

3° L'expression

$$C_1\varepsilon_1 + C_2\varepsilon_2 + \ldots + C_n\varepsilon_n$$

peut être rendue aussi petite que l'on veut.

Ces conditions étant supposées remplies, l'identité supposée est évidemment impossible, puisque la somme d'un entier non nul et d'une fraction proprement dite ne peut être égale à zéro.

3. Notre démonstration exige l'emploi d'un certain symbole h^r et d'un polynome $\varphi(x)$.

Le symbole h^r.

h^r n'est autre chose que $1.2.3 \ldots r = r!$; par l'emploi de ce symbole, on peut écrire

$$e^x = 1 + \frac{x}{h} + \frac{x^2}{h^2} + \cdots + \frac{x^n}{h^n} + \cdots$$

Il n'a pas d'autre signification ; il sert uniquement à écrire sous une forme plus simple toute formule contenant des puissances et des factorielles.

Supposons donné un polynome *développé*

$$f(x) = \sum_r c_r x^r ;$$

nous représentons par $f(h)$ et nous écrivons sous la forme

$$\sum_r c_r h^r$$

la somme

$$c_1 . 1 + c_2 . 2\,! + c_3 . 3\,! + \cdots + c_n n\,!$$

Supposons que le polynome $f(x)$ ne soit pas développé. Calculer $f(h)$, c'est développer ce polynome par rapport aux puissances de h et remplacer ensuite h^r par $r!$. C'est ainsi que

$$f(k+h) = \sum_r c_r (k+h)^r = \sum_r c'_r h^r = \sum_r c'_r . r\,!$$

Le polynome $\varphi(x)$.

Considérons le polynome remarquable

$$\varphi(x) = x^{p-1} \frac{[(1-x)(2-x) \ldots (n-x)]^p}{(p-1)\,!}.$$

p est un nombre premier, n le degré de l'équation algébrique à laquelle satisfait par hypothèse le nombre e. Nous supposerons p supérieur à n et à $|C_0|$, et plus tard nous le ferons croître au-delà de toute limite.

On aura une image géométrique de ce polynome en construisant la courbe

$$y = \varphi(x).$$

Aux points $x = 1, 2, \ldots, n$ elle admet l'axe des x comme tangente d'inflexion, puisqu'elle le rencontre en un nombre impair de points, tandis qu'à l'origine, elle le touche sans inflexion. Pour les valeurs de x comprises entre 0 et n, elle reste dans le voisinage de l'axe des x : pour des valeurs plus grandes de x, elle s'en écarte indéfiniment.

Propriétés du polynome $\varphi(x)$.

I. *x étant supposé donné et p croissant au-delà de toute limite, $\varphi(x)$ tend vers zéro, et de même la somme des valeurs absolues de ses termes.*

Posons $u = x(1-x)\ldots(n-x)$; on peut écrire

$$\varphi(x) = \frac{u^{p-1}}{(p-1)!}\,\frac{u}{x},$$

qui, pour p infini, tend évidemment vers 0.

Pour avoir la somme des valeurs absolues de $\varphi(x)$, il suffit de remplacer $-x$ par $|x|$ dans la forme non développée de $\varphi(x)$. La seconde partie de la proposition se démontre alors comme la première.

II. *h étant un nombre entier, $\varphi(h)$ est un nombre entier, non divisible par p, et par suite différent de zéro.*

Développons $\varphi(x)$ par rapport aux puissances croissantes de x, en remarquant que les termes de degré le moins et le plus élevé sont respectivement de degré $p-1$ et $np+p-1$. On aura

$$\varphi(x) = \sum_{r=p-1}^{r=np+p-1} c_r x^r = \frac{c_{p-1}x^{p-1}}{(p-1)!} + \frac{c_p x^p}{(p-1)!} + \cdots \pm \frac{x^{np+p-1}}{(p-1)!}.$$

Donc

$$\varphi(h) = \sum_{r=p-1}^{r=np+p-1} c_r h^r.$$

Abstraction faite du dénominateur $(p-1)!$ qui figure dans tous les termes, les coefficients c_r sont des nombres entiers. Ce dénominateur disparaît sitôt qu'on remplace h^r par $r!$, puisque la factorielle de moindre degré est

$$h^{p-1} = (p-1)!.$$

Tous les termes du développement, à partir du second, contiendront le facteur p. Quant au premier, il s'écrit

$$\frac{(1.2\ldots n)^p . (p-1)!}{(p-1)!} = (n!)^p,$$

et n'est certainement pas divisible par le nombre premier p, puisque, par hypothèse, p est un nombre plus grand que n.

Donc

$$\varphi(h) \equiv (n!)^p \qquad \text{mod. } p,$$

et par suite $\qquad \varphi(h) \not\equiv 0.$

$\varphi(h)$ est d'ailleurs un très grand nombre ; calculons son terme de degré le plus élevé ; c'est

$$\frac{(np+p-1)!}{(p-1)!} = p(p+1)\cdots(np+p-1).$$

III. *h étant un entier, et k l'un des nombres*

$$1,\ 2,\ \ldots,\ n,$$

$\varphi(h+k)$ est un nombre entier divisible par p.

On a

$$\varphi(h+k) = \sum_r c_r(h+k)^r = \sum_r c'_r h^r,$$

formule dans laquelle on ne doit remplacer h^r par $r!$ qu'après avoir ordonné le développement par rapport aux puissances croissantes de h.

D'après les règles indiquées pour le calcul symbolique, on a d'abord

$$\varphi(h+k) = (h+k)^{p-1}\frac{[(1-k-h)(2-k-h)\cdots(-h)\cdots(n-k-h)]^p}{(p-1)!}.$$

k ayant l'une des valeurs $1, 2, \ldots, n$, un des facteurs du crochet se réduit à $-h$: par suite, le terme du moindre degré en h dans le développement est de degré p. On peut donc écrire

$$\varphi(h+k) = \sum_{r=p}^{r=np+p-1} c'_r h^r.$$

Les coefficients ont encore pour numérateurs des nombres

entiers et pour dénominateur $(p-1)!$. Ce dénominateur disparaît sitôt qu'on remplace h^r par $r!$ Mais, cette fois-ci, tous les termes du développement sont divisibles par p ; en effet, le premier s'écrit

$$\frac{(-1)^{kp}.k^{p-1}.(k-1)!(n-k)!^p.p!}{(p-1)!} = (-1)^{kp}.k^{p-1}(k-1)!(n-k)!^p.p.$$

$\varphi(h+k)$ est donc divisible par p.

4. Démontrons maintenant que l'identité

$$F(e) = C_0 + C_1 e + C_2 e^2 + \ldots + C_n e^n = 0$$

est impossible.

Multiplions les deux membres par $\varphi(h)$; il vient

$$\varphi(h).F(e) = C_0\varphi(h) + C_1\varphi(h)e + \cdots + C_n\varphi(h)e^n = 0.$$

Cherchons ensuite à décomposer un terme quelconque $C_k\varphi(h)e^k$ en un entier et une fraction. On a

$$e^k.\varphi(h) = e^k \sum_r c_r h^r.$$

Ayant égard au développement en série de e^k, un terme quelconque de cette somme, abstraction faite du coefficient c_r, a la forme

$$e^k.h^r = h^r + \frac{h^r.k}{1} + \frac{h^r.k^2}{2!} + \cdots + \frac{h^r.k^r}{r!} + \frac{h^r.k^{r+1}}{(r+1)!} + \cdots.$$

On doit y remplacer h^r par $r!$, ou, ce qui revient au même, par l'une des quantités

$$rh^{r-1}, \quad r(r-1)h^{r-2}, \quad \ldots, \quad r(r-1)\ldots 3.h^2, \quad r(r-1)\ldots 2.h\,;$$

si en même temps on simplifie les fractions successives, il vient

$$e^k.h^r = h^r + \frac{r}{1}\cdot h^{r-1}.k + \frac{r(r-1)}{2!}h^{r-2}k^2 + \cdots$$

$$+ \frac{r(r-1)}{2!}h^2k^{r-2} + \frac{r}{1}hk^{r-1} + k^r$$

$$+ k^r\left[\frac{k}{r+1} + \frac{k^2}{(r+1)(r+2)} + \cdots\right].$$

La première ligne a même forme que le développement de $(h+k)^r$; dans la parenthèse de la seconde ligne se trouve la série

$$0+\frac{k}{r+1}+\frac{k^2}{(r+1)(r+2)}+\cdots,$$

dont les termes sont respectivement inférieurs à ceux de la série

$$e^k=1+\frac{k}{1}+\frac{k^2}{2!}+\cdots.$$

La seconde ligne peut donc se représenter par une expression de la forme

$$q_{r,k}\,.\,e^k\,.\,k^r,$$

q_{rk} étant une fraction proprement dite.

Faisons la même décomposition pour chaque terme de la somme

$$e^k\sum c_r h^r:$$

elle prend la forme

$$e^k\sum_r c_r h^r=\sum_r c_r(h+k)^r+e^k\sum q_{r,k}c_r k^r.$$

La première partie de cette somme n'est autre que $\varphi(h+k)$: c'est donc (propriété III) un nombre entier divisible par p. D'autre part (propriété I)

$$\varphi(k)=\sum c_r k^r$$

tend vers 0 quand p devient infini : il en est donc de même *a fortiori* de

$$e^k\sum_r q_{r,k}c_r k^r=\varepsilon_k.$$

Le terme considéré $C_k e^k \varphi(h)$ est donc bien sous la forme d'un entier $C_k\varphi(h+k)$ et d'une quantité $C_k\varepsilon_k$ qui, par un choix convenable de p, peut être rendue aussi petite qu'on le veut.

En procédant de même pour tous les termes, il vient

finalement

$$F(e)\varphi(h) = C_0\varphi(h) + C_1\varphi(h+1) + \ldots + C_n\varphi(h+n)$$
$$+ C_1\varepsilon_1 + C_2\varepsilon_2 + \ldots + C_n\varepsilon_n.$$

Il est maintenant facile d'achever la démonstration. Tous les nombres de la première ligne, à partir du second, sont divisibles par p; pour le premier le facteur C_0 est en valeur absolue inférieur à p; $\varphi(h)$ n'est pas divisible par p; donc $C_0\varphi(h)$ n'est pas divisible par le nombre premier p. Par conséquent la somme des nombres de la première ligne n'est pas nulle.

Les nombres de la seconde ligne sont en nombre fini; chacun d'eux peut être rendu plus petit que tout nombre donné par un choix convenable de p; il en est donc de même de leur somme.

Un nombre entier non nul et une fraction ne pouvant donner pour somme zéro, l'identité supposée est donc impossible.

La transcendance de e, ou encore le *théorème de M. Hermite* est donc démontré.

CHAPITRE IV

La transcendance du nombre π.

1. La démonstration de la transcendance du nombre π est due à M. Lindemann. C'est une extension de celle donnée par M. Hermite pour le nombre e.

Dans le chapitre précédent, on a montré que le nombre e ne pouvait vérifier une identité de la forme

$$C_0 + C_1 e + C_2 e^2 + \dots + C_n e^n = 0.$$

M. Lindemann démontre l'impossibilité d'une identité analogue : seulement, à la place des puissances e, e^2, ... il introduit des sommes de la forme

$$e^{k_1} + e^{k_2} + \dots + e^{k_N},$$

$$e^{l_1} + e^{l_2} + \dots + e^{l_{N'}},$$

. . . .

Les nombres $k_1, k_2, \dots, k_N$ sont les racines d'une même équation algébrique, à coefficients entiers du degré N : de même les nombres $l_1, l_2, \dots, l_{N'}$ sont les racines d'une équation de degré N', etc. Ces racines peuvent d'ailleurs être imaginaires.

Le théorème général de M. Lindemann peut donc s'énoncer sous la forme suivante :

Le nombre e ne peut vérifier une identité de la forme

$$(1)\quad C_0 + C_1(e^{k_1} + e^{k_2} + \dots + e^{k_N}) + C_2(e^{l_1} + e^{l_2} + \dots + e^{l_{N'}}) + \dots = 0,$$

les coefficients C_i étant entiers, et les exposants d'une même parenthèse étant les racines réelles ou imaginaires d'une même équation algébrique à coefficients entiers.

Soit

$$ax^N + a_1 x^{N-1} + \dots + a_N = 0$$

l'équation admettant pour racines les exposants k_i ;

$$bx^{N'} + b_1x^{N'-1} + \cdots + b_{N'} = 0,$$

celle qui admet pour racines les exposants l_i. Ces équations ne sont pas nécessairement irréductibles, ni leurs premiers coefficients égaux à l'unité ; les fonctions symétriques de leurs racines, qui seules se présenteront dans nos développements ultérieurs, ne sont donc pas nécessairement des nombres entiers.

Pour n'avoir que des nombres entiers, il suffira de considérer les fonctions symétriques des nombres

$$ak_1, ak_2, \ldots, ak_N,$$

$$bl_1, bl_2, \ldots, bl_{N'}, \text{ etc.}$$

On voit facilement que ces nombres sont racines des équations

$$y^N + a_1y^{N-1} + a_1ay^{N-2} + \cdots + a_Na^{N-1} = 0,$$

$$y^{N'} + b_1y^{N'-1} + b_1by^{N'-2} + \cdots + b_{N'}b^{N'-1} = 0, \text{ etc.}$$

les fonctions symétriques rationnelles des racines de ces équations sont évidemment des nombres entiers.

Cela posé, la marche de la démonstration est la même que pour le théorème de M. Hermite.

On suppose vraie l'identité (1) ; on multiplie ses deux membres par un même nombre M ; on décompose chaque somme telle que

$$M(e^{k_1} + e^{k_2} + \cdots + e^{k_N})$$

en une partie entière et une fraction, telle que

$$M(e^{k_1} + e^{k_2} + \cdots + e^{k_N}) = M_1 + \varepsilon_1,$$

$$M(e^{l_1} + e^{l_2} + \cdots + e^{l_{N'}}) = M_2 + \varepsilon_2,$$

. . . .

Notre identité devient alors

$$C_0M + C_1M_1 + C_2M_2 + \cdots + C_1\varepsilon_1 + C_2\varepsilon_2 + \cdots = 0.$$

On montrera, par un choix convenable de M, que la somme des nombres de la première ligne représente un

entier non divisible par un certain nombre premier p, et par suite différent de zéro; que la partie fractionnaire au contraire peut être rendue plus petite que tout nombre donné; on tombe alors sur la même contradiction que précédemment.

2. Nous nous servirons encore du symbole h^{ν}, et d'une certaine fonction $\psi(x)$.

Le polynome $\psi(x)$.

Ce polynome est une généralisation du polynome $\varphi(x)$ employé dans le chapitre précédent. On pose

$$\psi(x) = \frac{x^{p-1}}{(p-1)!}[(k_1 - x)(k_2 - x) \dots (k_N - x)]^p . a^{Np} . a^{N'}(a^{Np}) \dots$$
$$\times [(l_1 - x)(l_2 - x) \dots (l_{N'} - x)]^p b^{N'p} . b^{N'p} b^{N'p} \dots$$
$$\times \dots\dots\dots\dots\dots\dots$$

p est un nombre premier, supérieur en valeur absolue à chacun des nombres

$$C_0,\ a,\ b,\ \dots\ a_N,\ b_{N'},\ \dots;$$

nous le ferons même croître indéfiniment. Quant aux facteurs a^{Np}, $b^{N'p}$, ..., nous les avons introduits afin de trouver dans le développement de $\psi(x)$ des fonctions symétriques des quantités.

$$ak_1,\ ak_2,\ \dots,\ ak_N,$$
$$bl_1,\ bl_2,\ \dots,\ bl_{N'}.$$
$$\dots\dots\dots$$

c'est-à-dire des nombres rationnels et entiers.

Plus loin nous aurons à développer les quantités

$$\sum_{\nu} \psi(k_\nu + h), \qquad \sum_{\nu} \psi(\lambda_\nu + h).$$

La présence des mêmes facteurs sera encore nécessaire, si on veut que les coefficients de ces développements aient pour numérateurs des nombres entiers.

Propriétés de la fonction $\psi(x)$.

I. *$\psi(h)$ est un nombre entier, non divisible par p, et par suite différent de zéro.*

En ordonnant $\psi(h)$ par rapport aux puissances croissantes de h, il vient

$$\psi(h) = \sum_{r=p-1}^{r=Np+N'p+\cdots+p-1} c_r h^r.$$

Dans ce développement tous les coefficients ont pour numérateurs des nombres entiers et pour dénominateur $(p-1)!$.

Le coefficient du premier terme h^{p-1} s'écrit par exemple

$$\begin{aligned}&\frac{1}{(p-1)!}(ak_1.ak_2\ldots ak_N)^p.a^{N'p}a^{N''p}\ldots\\&\qquad\times(bl_1.bl_2\ldots bl_{N'})^p.b^{Np}b^{N''p}\ldots\\&\qquad\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\&=\frac{1}{(p-1)!}(-1)^{Np+N'p+\cdots}.(a_N a^{N-1})^p.a^{N'p}.a^{N''p}\ldots(b_{N'}b^{N'-1})^p.b^{Np}b^{N''p}\ldots\end{aligned}$$

Si dans ce terme nous remplaçons h^{p-1} par $(p-1)!$, le dénominateur disparait. D'après les hypothèses faites sur le nombre premier p, aucun facteur de ce produit n'est divisible par p, et par suite il en est de même du produit.

Le second terme $C_p h^p$ devient de même un nombre entier quand on remplace h^p par $p!$; mais le facteur p se conserve, et il en sera de même pour tous les termes suivants. Donc la somme $\psi(h)$ est un entier non divisible par p.

II. *x ayant une valeur finie donnée, et p augmentant indéfiniment, le polynome*

$$\psi(x) = \sum_r c_r x^r$$

tend vers 0, de même que la somme des modules de ses termes.

On a
$$\psi(x) = \sum c_r x^r$$

$$\begin{aligned}&=\frac{x^{p-1}}{(p-1)!}[a^N.a^{N'}\ldots(k_1-x)(k_2-x)\ldots(k_N-x)\\&\qquad\times b^N b^{N'}\ldots(l_1-x)(l_2-x)\ldots(l_{N'}-x)\\&\qquad\times\ldots\ldots\ldots\ldots\ldots\ldots]^p.\end{aligned}$$

Désignons le crochet par K : il vient alors

$$\psi(x) = \frac{(xK)^{p-1}}{(p-1)!} K,$$

et cette quantité tend évidemment vers 0, quand p croît indéfiniment.

Ce raisonnement reste évidemment valable quand on remplace chaque terme de $\psi(x)$ par son module.

III. *L'expression* $\sum_{\nu=1}^{\nu=N} \psi(k_\nu + h)$ *est un nombre entier divisible par* p.

On a

$$\psi(k_\nu + h) = \frac{a^p (k_\nu + h)^{p-1}}{(p-1)!} b^{Np} . b^{N'p} \ldots$$
$$\times a^{(N-1)p} [(k_1 - k_\nu - h) \ldots (-h) \ldots (k_N - k_\nu - h)]^p$$
$$\times a^{N'p} . b^{N'p} [(l_1 - k_\nu - h) \ldots\ldots\ldots (l_{N'} - k_\nu - h)]^p$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Le ν^e facteur du crochet de la seconde ligne se réduit à $-h$; le terme de degré le moins élevé en h dans le développement est donc h^p. Par suite

$$\psi(k_\nu + h) = \sum_{i=p}^{i=Np+N'p+\cdots+p-1} c_i^\nu h^i.$$

d'où

$$\sum_{\nu=1}^{\nu=N} \psi(k_\nu + h) = \sum_{i=p}^{i=Np+N'p+\cdots+p-1} C_i h^i.$$

Les numérateurs des coefficients C_i sont des nombres rationnels et entiers ; car ce sont des fonctions symétriques entières des quantités

$$ak_1 \ldots ak_N,$$
$$bl_1 \ldots bl_{N'},$$
$$\ldots\ldots\ldots ;$$

leur dénominateur est égal à $(p-1)!$.

Remplaçons maintenant h^r par $r!$; le dénominateur disparaît dans tous les coefficients ; mais le facteur p se conserve au numérateur ; la somme est donc bien un nombre entier divisible par p.

Il en sera évidemment de même pour

$$\sum_{\nu=1}^{\nu=N'} \psi(l_\nu + h) \ \ldots$$

Nous avons ainsi trois propriétés de $\psi(x)$, analogues à celles démontrées pour $\varphi(x)$ à l'occasion du théorème de M. Hermite.

3. Revenons maintenant à la démonstration de notre théorème. Il s'agit de montrer que l'identité

$$(1) \quad C_0 + C_1(e^{k_1} + e^{k_2} + \cdots + e^{k_N}) + C_2(e^{l_1} + e^{l_2} + \cdots + e^{l_{N'}}) + \cdots = 0$$

est impossible.

A cet effet, multiplions ses deux membres par $\psi(h)$: elle devient

$$C_0\psi(h) + C_1[e^{k_1}\psi(h) + \cdots + e^{k_N}.\psi(h)]$$
$$+ C_2[e^{l_1}.\psi(h) + \cdots + e^{l_{N'}}.\psi(h)] + \cdots = 0.$$

Cherchons à décomposer chacune des parenthèses en un nombre entier et une fraction. L'opération sera un peu plus longue que précédemment, car k peut être une quantité complexe de la forme $k' + ik''$; soit $|k|$ son module $\sqrt{k'^2 + k''^2}$.

On a

$$e^k.\psi(h) = e^k \sum_r c_r h^r = \sum_r c_r.e^k h^r.$$

Le produit $e^k.h^r$ peut s'écrire, comme nous l'avons montré précédemment,

$$e^k.h^r = (h + k)^r + k^r\left[\frac{k}{r+1} + \frac{k^2}{(r+1)(r+2)} + \cdots\right].$$

Les modules des termes de la série

$$0 + \frac{k}{r+1} + \frac{k^2}{(r+1)(r+2)} + \cdots$$

sont respectivement inférieurs à ceux des termes de la série

$$e^k = 1 + \frac{k}{1} + \frac{k^2}{2\,!} + \cdots$$

Il en résulte

$$\text{mod.} \left| \frac{k}{r+1} + \frac{k^2}{(r+1)(r+2)} + \cdots \right| < e^{|k|},$$

ou bien

$$\frac{k}{r+1} + \frac{k^2}{(r+1)(r+2)} + \cdots = q_{r,k}.e^{|k|},$$

$q_{r,k}$ étant une quantité complexe dont le module est inférieur à l'unité.

On peut donc écrire

$$e^k.\psi(h) = \sum_r c_r e^k.h^r = \sum_r c_r(h+k)^r + \sum_r c_r q_{r,k}.k^r.e^{|k|}$$

$$= \psi(h+k) + \sum_r c_r q_{r,k} k^r e^{|k|}.$$

Affectons dans cette égalité k successivement des indices 1, 2, ..., N, et faisons la somme ; il vient

$$e^{k_1}.\psi(h) + e^{k_2}.\psi(h) + \cdots + e^{k_N}.\psi(h)$$

$$= \sum_{\nu=1}^{\nu=N} \psi(k_\nu + h) + \sum_{\nu=1}^{\nu=N} \left\{ e^{|k_\nu|} \sum_r c_r.k_\nu^r.q_{r,k_\nu} \right\}.$$

Procédons de même pour toutes les autres sommes ; le premier membre de notre identité prend alors la forme

$$(2)\quad \begin{aligned} &C_0\psi(h) + C_1\sum_{\nu=1}^{\nu=N} \psi(k_\nu + h) + C_2\sum_{\nu=1}^{\nu=N'} \psi(l_\nu + h) + \cdots \\ &+ C_1\sum_{\nu=1}^{\nu=N}\sum_r e^{|k_\nu|}.c_r.k_\nu^r.q_{r,k_\nu} + C_2\sum_{\nu=1}^{\nu=N'}\sum_r e^{|l_\nu|}.c_r.l_\nu^r.q_{r,l_\nu} + \cdots = 0. \end{aligned}$$

D'après la propriété II, on peut rendre $\sum_r |c_r k^r|$ plus petit que tout nombre donné, en choisissant p suffisamment grand. Comme

$$\text{mod. } q_{r,k} < 1,$$

il en sera *a fortiori* de même de

$$\sum_r c_r k^r . q_{r,k},$$

et par suite aussi de

$$\sum_{\nu=1}^{\nu=N} \sum_r c_r k_\nu^r . q_{r,k_\nu} e^{|k_\nu|}.$$

Comme le nombre des coefficients C est limité, la somme qui figure dans la deuxième ligne de l'identité (2) peut être rendue aussi petite que l'on voudra.

Les nombres de la première ligne sont, à partir du second, tous divisibles par p (Pr. III) : le premier nombre $C_0\psi(h)$ ne l'est pas (Pr. I). La somme des nombres de la première ligne n'est donc pas divisible par p, et par suite elle est différente de zéro. La somme d'un nombre entier et d'une fraction ne peut être nulle : l'identité (2) est donc impossible et par suite aussi l'identité (1).

4. Voici maintenant une proposition plus générale que la précédente, mais dont la démonstration est une conséquence immédiate de la première. Pour cette raison nous l'appellerons le

Corollaire de M. Lindemann.

Le nombre e ne peut vérifier une identité de la forme

$$C'_0 + C'_1 e^{k_1} + C'_2 e^{l_1} + \ldots = 0, \quad (3)$$

dans laquelle les coefficients sont des nombres entiers, et les exposants des nombres algébriques quelconques.

Pour le démontrer, soient

$$k_2, k_3, \dots, k_N$$

les autres racines de l'équation algébrique à laquelle satisfait k_1 ; de même soient

$$l_2, \dots, l_{N'}$$

les autres racines de l'équation à laquelle satisfait l_1, etc.

Formons tous les polynomes qu'on peut déduire de (3) en remplaçant k_1 successivement par les racines connexes $k_2, \dots$, l_1 par les racines $l_2 \dots$; faisons le produit de toutes les expressions ainsi formées, on aura

$$\prod_{\alpha, \beta, \dots} \{ C'_0 + C'_1 e^{\alpha} + C'_2 e^{\beta} + \cdots \} \left[\begin{array}{l} \alpha = k_1, k_2, \dots, k_N \\ \beta = l_1, l_2, \dots, l_{N'} \\ \dots\dots\dots\dots \end{array} \right]$$

$$= C_0 + C_1 (e^{k_1} + e^{k_2} + \cdots + e^{k_N}) + C_2 (e^{k_1+k_2} + e^{k_1+k_3} + \cdots) + \cdots$$

$$+ C_3 (e^{k_1+l_1} + e^{k_1+l_2} + \cdots) + \cdots$$

Dans chaque parenthèse, les exposants sont formés symétriquement avec les quantités $k, l \dots$; ce sont donc encore les racines d'une équation algébrique à coefficients entiers. Notre produit a alors la forme supposée dans le théorème de M. Lindemann ; par suite il ne peut devenir nul. Aucun de ses facteurs ne peut donc l'être, ce qui démontre le corollaire.

5. Voici enfin une proposition encore plus générale :

Le nombre e ne peut vérifier une identité de la forme

$$C'_0 + C'_1 e^k + C'_2 e^\lambda + \dots = 0,$$

dans laquelle les coefficients aussi bien que les exposants sont des nombres algébriques quelconques.

Formons en effet tous les polynomes qu'on peut déduire du précédent en remplaçant chacune des racines C'_i par l'une des racines connexes

$$C_i^2, C_i^3, \dots, C_i^N ;$$

le produit des polynomes ainsi formés est

$$\prod_{\alpha,\beta,\gamma,\ldots} \left\{ C_0^\alpha + C_1^\beta e^h + C_2^\gamma e^k + \ldots \right\} \left[\begin{array}{l} \alpha = 1,\, 2,\, \ldots,\, N_0 \\ \beta = 1,\, 2,\, \ldots,\, N_1 \\ \gamma = 1,\, 2,\, \ldots,\, N_2 \\ \ldots\ldots\ldots \end{array} \right]$$

$$= C_0 + C_h e^h + C_k e^k + \ldots + C_{hh} e^{h+h} + C_{hk} e^{h+k} + \ldots$$

Les coefficients de ce polynome sont des fonctions symétriques des quantités

$$C_0^1,\ C_0^2,\ \ldots,\ C_0^{N_0},$$
$$C_1^1,\ C_1^2,\ \ldots,\ C_1^{N_1},$$
$$\ldots\ldots\ldots$$

et par suite ce sont des nombres rationnels. Nous retombons donc sur le corollaire démontré précédemment : cette expression ne peut être nulle ; il en est donc de même de chacun de ses facteurs.

6. De tous les théorèmes qui précèdent, il résulte que non seulement e n'est pas un nombre algébrique, mais que ce n'est même pas un nombre *interscendant*, si on appelle ainsi, avec Leibniz, les nombres de la forme x^λ, λ étant une irrationnelle algébrique. C'est donc un nombre transcendant d'ordre supérieur.

La réciproque suivante est maintenant évidente :

Si le nombre e vérifie une identité de la forme

$$C_0 + C_1 e^h + C_2 e^k + \ldots = 0,$$

il est impossible que tous les coefficients et tous les exposants soient des nombres algébriques.

7. *Transcendance du nombre π.* — Nous avons déjà rappelé que le nombre e vérifie l'équation remarquable

$$1 + e^{i\pi} = 0.$$

Les coefficients de cette équation sont algébriques ; donc l'exposant $i\pi$ ne l'est pas (6) ; donc le nombre π est transcendant.

8. Considérons la fonction

$$y = e^x;$$

on sait que

$$1 = e^0;$$

et il semble que cette identité soit en contradiction avec notre théorème. Il n'en est rien ; il suffit en effet de remarquer que nous avons implicitement exclu le cas de l'exposant nul ; dans ce cas, la fonction $\psi(x)$ perdrait ses principales propriétés, et nos conclusions ne seraient plus exactes.

Excluons donc ce cas particulier ($x = 0$, $y = 1$) : le théorème de M. Lindemann prouve alors que, dans l'équation $y = e^x$, y et x, c'est-à-dire *le nombre et son logarithme ne peuvent pas être algébriques simultanément*. A une valeur algébrique de x correspond une valeur transcendante de y et réciproquement. C'est là évidemment une propriété très remarquable.

Construisons la courbe $y = e^x$, et supposons marqués tous les points algébriques du plan, c'est-à-dire tous les points dont les deux coordonnées sont des nombres algébriques ; la courbe passe entre eux, sans en contenir aucun, sauf le point $x = 0$, $y = 1$. Le théorème reste d'ailleurs vrai, même quand x et y prennent des valeurs imaginaires. La courbe exponentielle est donc une courbe transcendante, et cela dans un sens beaucoup plus élevé qu'on n'a coutume de le penser.

9. Une autre conséquence du corollaire de M. Lindemann est la transcendance de la courbe

$$y = \text{arc} \sin x$$

et de toutes les autres courbes analogues.

La fonction $y = \text{arc} \sin x$ est la fonction implicite définie par l'équation

$$2ix = e^{iy} - e^{-iy};$$

les coefficients de cette équation sont algébriques, si x est un nombre algébrique. Donc y n'est pas algébrique. Il y a bien entendu exception pour $x = 0$, $y = 0$.

On peut donc énoncer sous forme géométrique la proposition suivante :

La courbe $y = \text{arc} \sin x$ ne passe par aucun point du plan dont les deux coordonnées sont des nombres algébriques.

CHAPITRE V

L'Intégraphe et la construction géométrique de π.

1. Le théorème de M. Lindemann démontre la transcendance du nombre π; ainsi se trouve démontrée l'impossibilité de la quadrature du cercle, non seulement au sens où l'entendaient les anciens, mais d'une manière beaucoup plus générale.

Il est impossible de construire π avec la règle et le compas; il n'existe même pas de courbe d'ordre supérieur, définie par une équation algébrique, pour laquelle π soit l'ordonnée correspondant à une valeur rationnelle de l'abscisse.

Une véritable construction géométrique de π ne peut donc être effectuée qu'à l'aide d'une courbe transcendante. Comme d'ailleurs il s'agit d'une véritable construction, il faut posséder un appareil transcendant permettant de tracer la courbe en question d'un trait continu.

2. Cet appareil, c'est l'*intégraphe*, qui a été récemment inventé et décrit par un ingénieur russe, M. Abdank-Abakanowicz, et construit par M. Coradi à Zurich.

Cet instrument permet de tracer la *courbe intégrale*

$$Y = F(x) = \int f(x)\,dx,$$

quand on connaît la courbe différentielle

$$y = f(x).$$

A cet effet, on conduit l'intégraphe de telle manière que la *pointe directrice* décrive la courbe différentielle : une autre pointe, la *pointe traçante* décrit alors la courbe inté-

grale. Nous renvoyons au mémoire original (en allemand chez Teubner, 1889; en français chez Gauthier-Villars) pour la description de cet ingénieux instrument.

Indiquons seulement son principe. Étant donné un point (x, y) de la courbe différentielle

$$y = f(x),$$

construisons le triangle auxiliaire, qui a pour sommets les points (x, y), $(x, 0)$, $(x - 1, 0)$. L'hypoténuse de ce triangle rectangle fait avec l'axe des x un angle dont la tangente est égale à y.

Cette hypoténuse est donc parallèle à la tangente à la courbe intégrale au point (X, Y), *correspondant au point* (x, y).

L'appareil devra donc être construit de telle façon, que la pointe traçante se déplace parallèlement à la direction variable de cette hypoténuse, pendant que la pointe directrice décrit la courbe différentielle. On réalise ce mouvement en reliant la pointe traçante à une roulette à arête vive, dont le plan, toujours vertical, est constamment parallèle à cette hypoténuse. Un poids presse cette roulette sur le papier, et par suite son point de contact ne peut se déplacer que dans la direction du plan de la roulette.

On utilise l'intégraphe ou intégrateur à calculer pratiquement des intégrales définies. Pour nous, il est particulièrement intéressant au point de vue de la construction géométrique de π.

3. Prenons comme courbe différentielle le cercle

$$x^2 + y^2 = r^2.$$

La courbe intégrale est alors

$$Y = \int_0^x \sqrt{r^2 - x^2}.dx = \frac{r^2}{2} \text{ arc sin } \frac{x}{r} + \frac{x}{2} \sqrt{r^2 - x^2}.$$

Cette courbe consiste en une suite de branches égales entre elles (*fig.* 17). Les points où elle rencontre l'axe OY ont pour ordonnées

$$0, \qquad \pm \frac{r^2\pi}{2}, \qquad \ldots;$$

sur les droites $X = \pm r$, les points d'intersection ont pour ordonnées

$$r^2 \frac{\pi}{4}, \qquad r^2 \frac{3\pi}{4}, \qquad \ldots\ldots$$

Si donc on suppose $r = 1$, les ordonnées de ces points

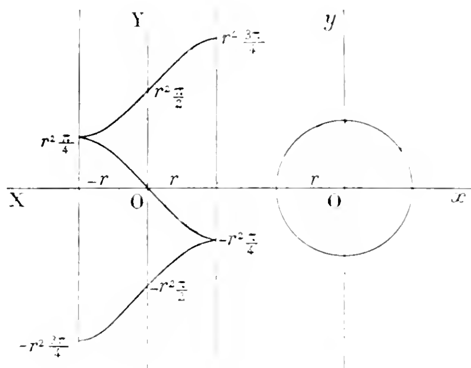


Fig. 17

d'intersection feront connaître le nombre π ou ses multiples.

Remarquons que le tracé de notre courbe n'a rien d'approximatif; l'appareil donne un dessin net et précis, surtout si on remplace le crayon par un tire-ligne.

Voilà donc une construction géométrique qui permet la quadrature du cercle. On voit de plus qu'elle la réalise dans l'ordre d'idées où s'étaient engagés les géomètres anciens; notre courbe intégrale n'est qu'une modification des quadratrices considérées par eux.

TABLE DES MATIÈRES

INTRODUCTION

PREMIÈRE PARTIE

POSSIBILITÉ DE LA CONSTRUCTION DES EXPRESSIONS ALGÉBRIQUES.

Chapitre I. — **Équations algébriques résolubles par radicaux carrés.**

Chapitre II. — **Le problème de Délos et la trisection d'un angle quelconque.**

CHAPITRE III. — La division du cercle en parties égales.

CHAPITRE IV. — Construction du polygone régulier de 17 côtés.

CHAPITRE V. — Généralités sur la construction des expressions algébriques.

DEUXIÈME PARTIE

LES NOMBRES TRANSCENDANTS ET LA QUADRATURE DU CERCLE.

CHAPITRE I. — Existence des nombres transcendants. Démonstration de M. Cantor.

Bar-le-Duc. — Imprimerie Comte-Jacquet.

